## SÉCURITÉ DES SYSTÈMES D'INFORMATION

# PROJET SÉCURITÉ 2K10

## GROUPE « ATTAQUE »

M2 « **S**ystèmes de **T**élécommunications & **R**éseaux **I**nformatiques »
IUP TOULOUSE – Université Paul SABATIER (TOULOUSE III)
S9 – Sécurité des systèmes d'information
Enseignant : Monsieur Philippe LATU

# Le groupe « ATTAQUE » 2k10

Benjamin **BAURY**
Yann **BECOURT**
Aymen **BEN HASSINE**
Thomas **BONNET**
Guillaume **COMET**
Ramatoulaye **DIALLO**
Alexandre **DUBOSC**

**GROUPE ATTAQUE 2k10**

Gérémy **GIULY**
Anaël **JALLET**
Gaël **JUIN**
Adil **NOUA**
Mickaël **POL**
Bastien **TOMAS**
Thomas **VIVIEN**

## À L'**ATTAQUE** !!!

**14 MEMBRES ISSUS DE DIVERSES FORMATIONS** : R&T, SRC, INFORMATIQUE, ETC…

**SPECIALITÉS** DIVERSES

**COMPLEMENTARITÉ** INTERESSANTE

**MOTIVATION** ÉNORME

STRI | Télécoms & Réseaux |

# Introduction

- Un projet étalé sur une durée de **deux mois** environ
- Trois groupes tirés au sort :
  - **ATTAQUE**, **DÉFENSE** et **AUDIT**
- Système de « **confrontations** » permettant de présenter le travail fourni
- Immersion dans le domaine de la sécurité informatique (**contexte entreprise**)

Projet encadré par **M. Philippe LATU**

STRI | Télécoms & Réseaux |

# Plan

- Présentation **chronologique**

AUTOUR DU GROUPE « ATTAQUE » 2010

PREMIÈRE CONFRONTATION

C'EST NOËL AVANT L'HEURE

DEUXIÈME CONFRONTATION

ULTIME CONFRONTATION

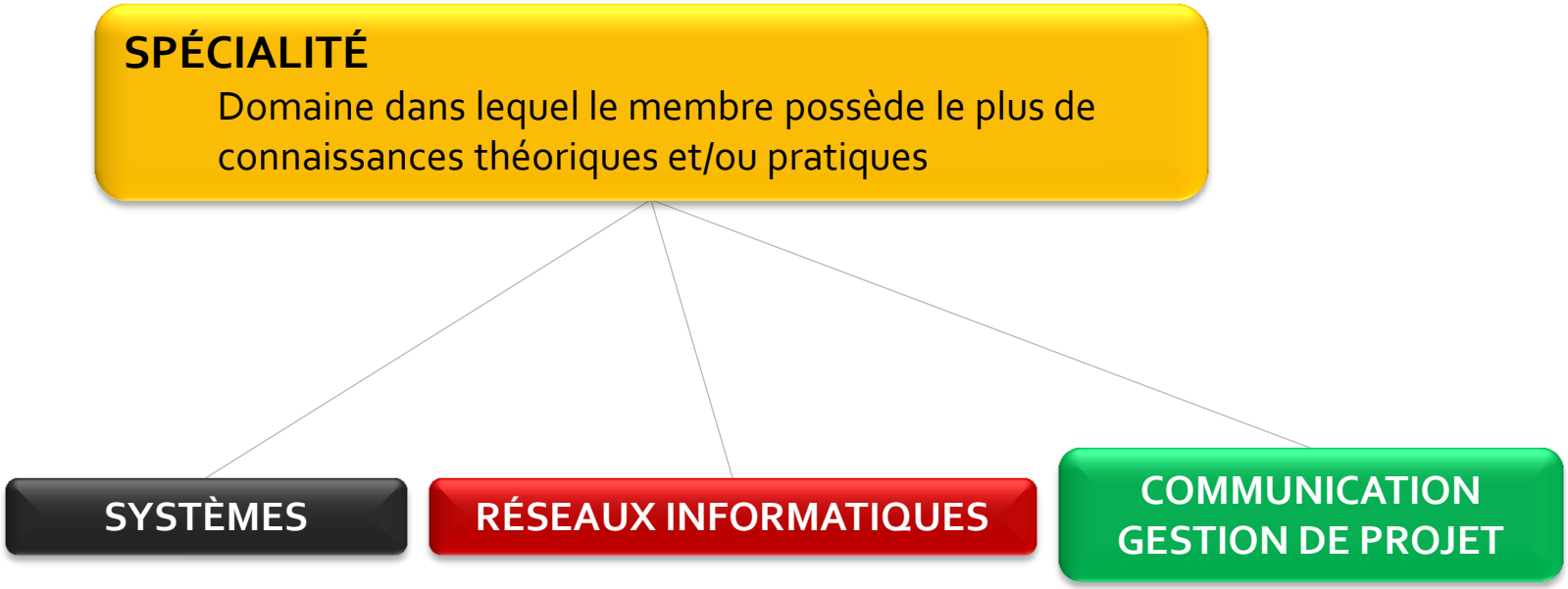
QUAND IL N'Y EN A PLUS…

BILAN

STRI | Télécoms & Réseaux |

# Autour du groupe « ATTAQUE »

- Une philosophie de travail adoptée dès le départ :
  - Prise en compte des envies et centres d'intérêts de chacun
    - Associations « **membre/spécialité** »

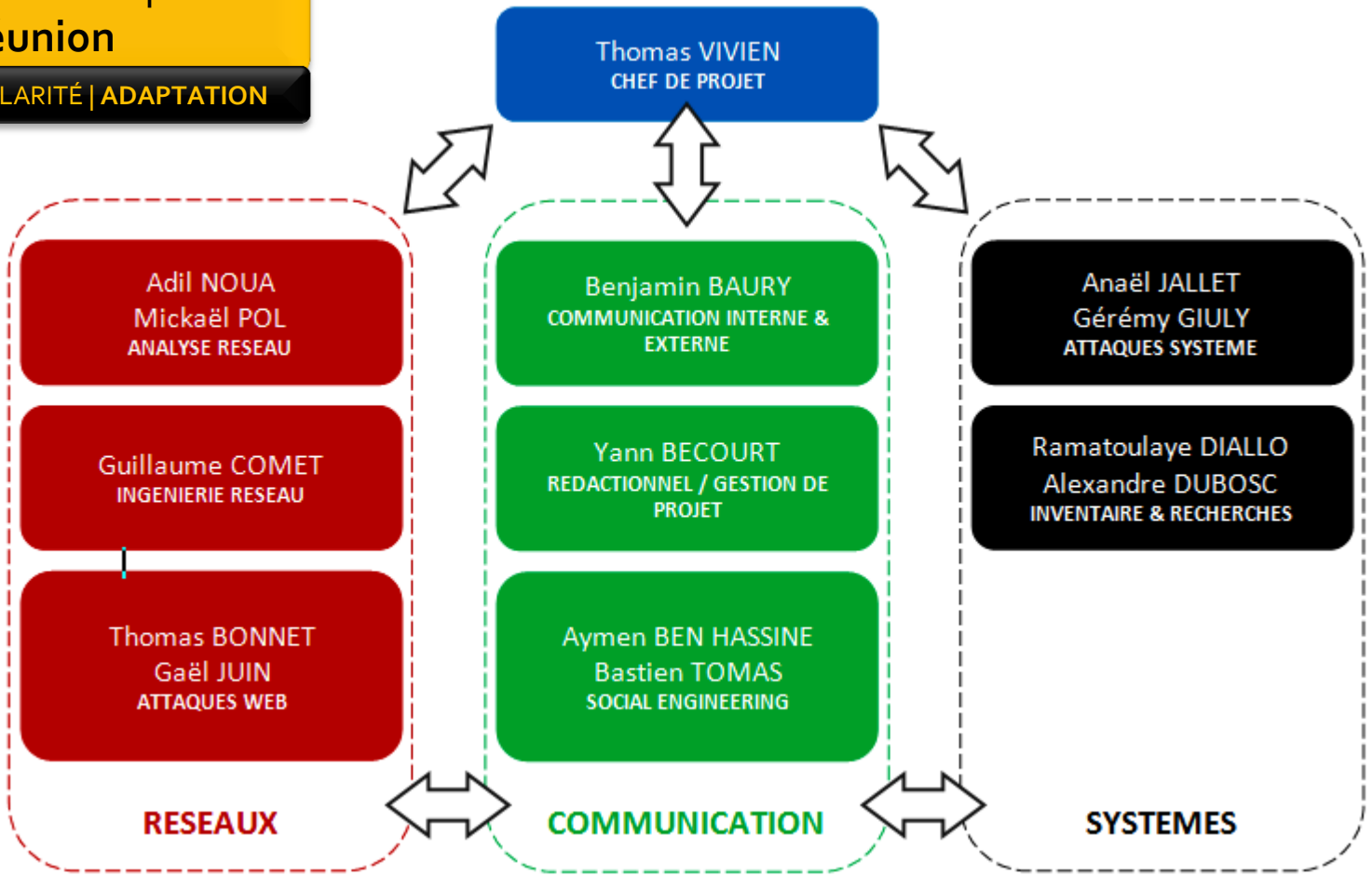



STRI Télécoms & Réseaux

# Autour du groupe « ATTAQUE »

Organigramme de départ
**vu en réunion**

SEGMENTATION | MODULARITÉ | **ADAPTATION**




« Rien n'est figé, tout évolue »

# Autour du groupe « ATTAQUE »

- Politique de communication :
  - **UN SEUL RESPONSABLE** : Benjamin BAURY (communication INTERNE et EXTERNE)
  - **DISCRÉTION** : éviter de parler du projet en dehors des réunions, par exemple
  - **EFFICACITÉ** : clarté des discours, compréhension des acteurs, etc…
  - **RÉUNIONS** : échange d'idées, organisation, plans, etc…
  - **USAGE DU MAIL** : communications ne contenant aucune information importante
  - **ÉCHANGES DE FICHIERS** : réunions (clé USB) ou conversation MSN **valide**

« Rien n'empêchait la défense ou l'audit de **nous attaquer !!!** »

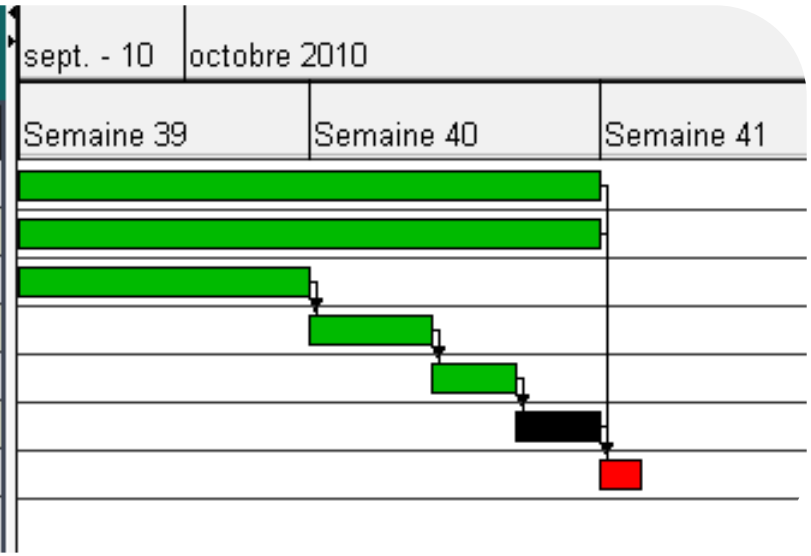
STRI | Télécoms & Réseaux |

# Autour du groupe « ATTAQUE »

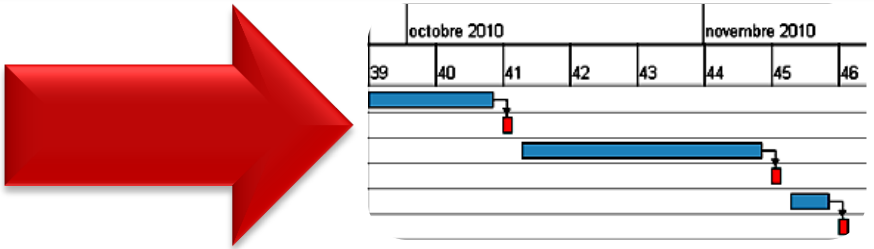
- Exemple de planification (confrontation n°01) :

GANTT project

| Nom | Date de début | Date de fin |
|---|---|---|
| Recherches générales (outils, etc...) | 27/09/10 | 11/10/10 |
| Récupération d'informations (Social Ing.) | 27/09/10 | 11/10/10 |
| Etude de la topologie réseau | 27/09/10 | 04/10/10 |
| Recherches des vulnérabilités | 04/10/10 | 07/10/10 |
| Conception de la boite à outils | 07/10/10 | 09/10/10 |
| Test et scénarisation | 09/10/10 | 11/10/10 |
| CONFRONTATION 01 | 11/10/10 | 12/10/10 |




Planification de base utilisée pour les différentes confrontations




STRI | Télécoms & Réseaux |

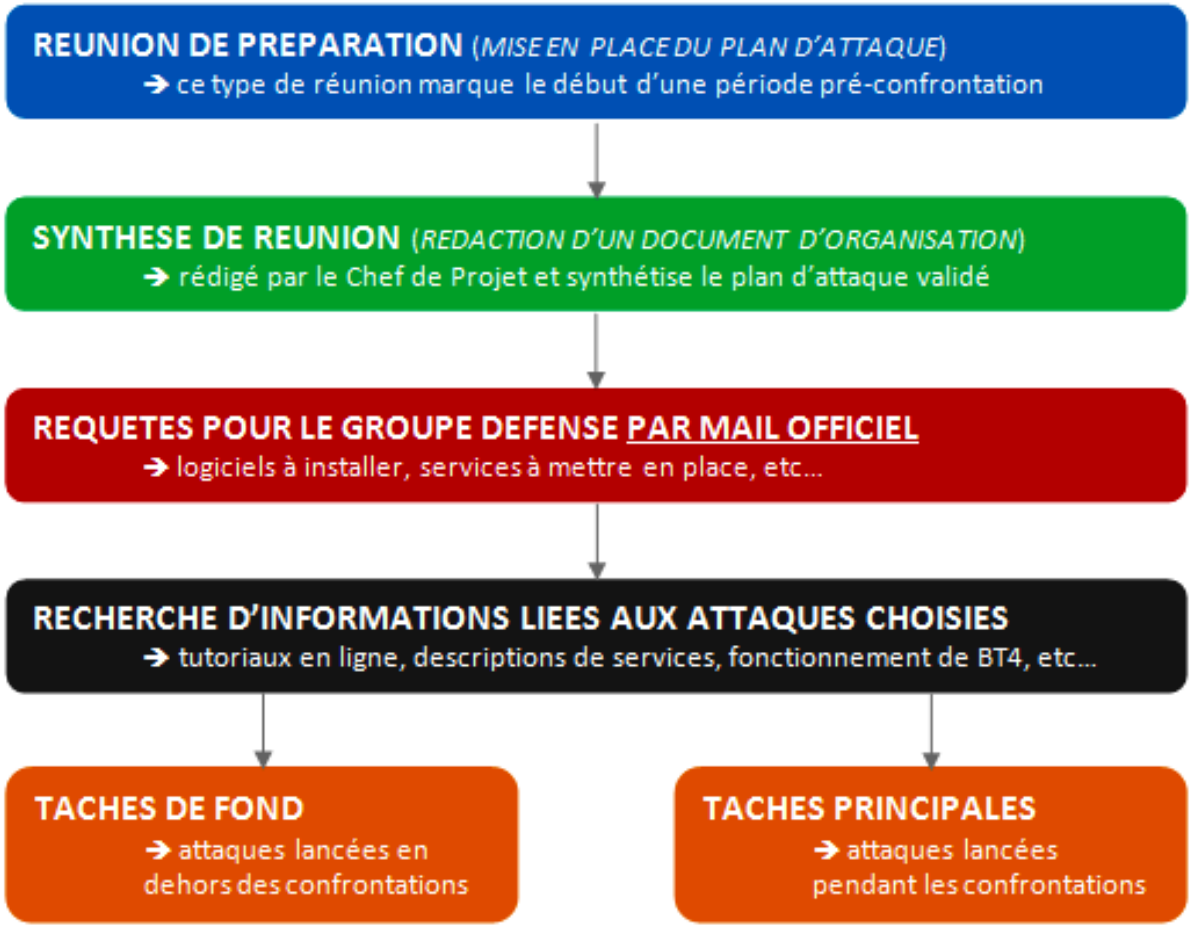
# Autour du groupe « ATTAQUE »

- Étude des anciens rapports (partie attaque ici) :


SPONSOR OFFICIEL :

# Autour du groupe « ATTAQUE »

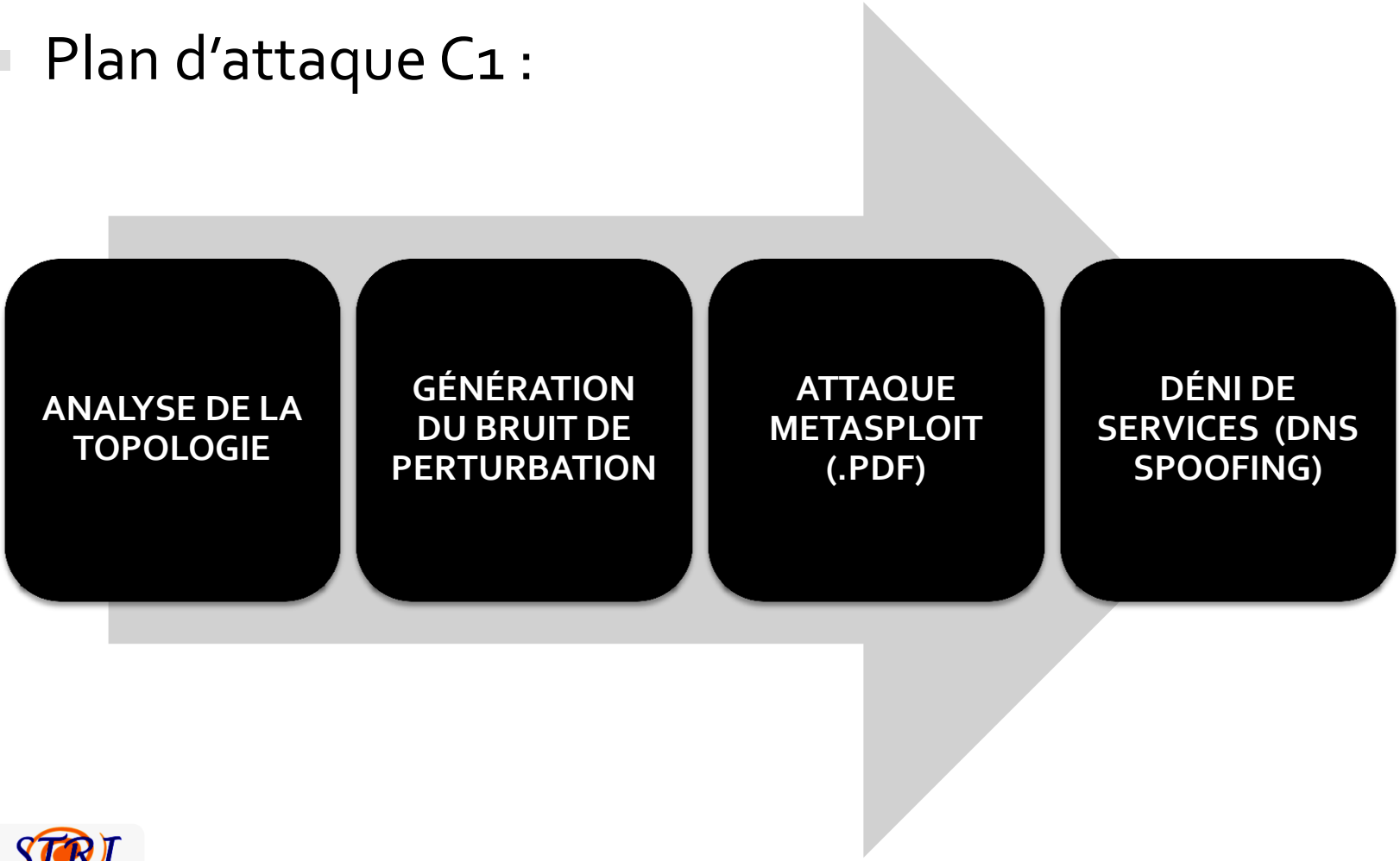
- Déroulement des phases d'attaque :




STRI Télécoms & Réseaux

# Première confrontation (C1)

- Plan d'attaque C1 :



# Première confrontation (C1)

- La communication :
  - Avis du groupe lors de la C1 : **mauvaise volonté flagrante de l'équipe de défense** (déploiements tardifs, retards, …)
  - Préconisations non respectées (installations demandées)

**« Veulent-ils gagner du temps OU sont-ils en train de nous tester ? »**

**MAIS**

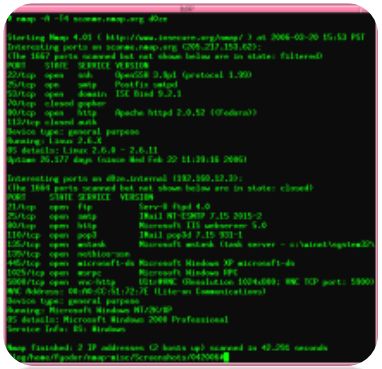
  - Demande de support : **opportunité d'attaque** pour nous !
  - Au niveau interne : **augmentation de l'indépendance des groupes de travail**

# Première confrontation (C1)

- L'analyse réseau : GÉNÉRALITÉS
  - RÔLE ➔ **collecte d'informations**
  - BUT ➔ **rassembler un maximum d'informations** :
    - Système d'exploitation (OS)
    - Adressage IP
    - Services activés
    - Autres

# Première confrontation (C1)

- L'analyse réseau : NMAP
  - Scanner de sécurité **le plus connu**
  - Détecte les ports ouverts
  - Composé d'**options** :
    - Informations de service
    - Version
    - OS
  - Résultats : **récupération des ports OUVERTS**



22 : **SSH** | 23 : **TELNET** | 25 : **SMTP** | 53 : **DNS** | 80 : **HTTP**
1720 : **H323** | 3001 : **NESSUS** | 5060 : **SERVEUR SIP** | 5061 : **SIP/TLS**

STRI Télécoms & Réseaux

# Première confrontation (C1)

- L'analyse réseau : NESSUS

  - Partie SERVEUR : **base de données**
  - Partie CLIENT : **ordonne au serveur de procéder aux tests**

  - Phase de TEST :
    - **Détection des machines vivantes sur le réseau**
    - **Scan des ports**
    - **Récupération d'informations**
      - Type et version des divers services
      - Connexion (SSH, TELNET) pour récupérer la liste des packages installés
    - **Attaques susceptibles d'être destructrices**
    - **Dénis de service** (contre les logiciels visés)
    - Dénis de service contre la machine ou les équipements réseaux intermédiaires

# Première confrontation (C1)

- L'analyse réseau : NESSUS (résultats)


## 172.30.0.1

**Scan Time**

| | |
|---|---|
| Start time : | Mon Oct 11 01:45:44 2010 |
| End time : | Mon Oct 11 01:48:47 2010 |

**Number of vulnerabilities**

| | |
|---|---|
| Open ports : | 13 |
| High : | 0 |
| Medium : | 2 |
| Low : | 31 |

**Remote host information**

| | |
|---|---|
| Operating System : | Linux Kernel 2.6.35.5 |
| NetBIOS name : | |
| DNS name : | |

STRI Télécoms & Réseaux

# Première confrontation (C1)

- L'analyse réseau : SNMP & DNS
  - **SNMP**
    - SNMP Agent Default Community Name
    - Non exploitée
  - **DNS**
    - DNS SNOOPING
      - Récupération cache DNS
      - Script NMAP
      - Résultats : NÉANT

# Première confrontation (C1)

- DNS SPOOFING :
  - Utilisation d'ETTERCAP (couteau suisse du sniff / injection Ethernet)
  - Utilisation du serveur placé dans le réseau public (172.30.0.4)

```
ettercap –T –q –i
etho –P dns_spoof –M arp 172.30.0.1 //
```

  - Interception de toutes les requêtes DNS et redirection vers le serveur Web hébergé en local
  - Impossible de rediriger vers des pages hébergées sur un réseau extérieur du fait du proxy SQUID sur Cooper

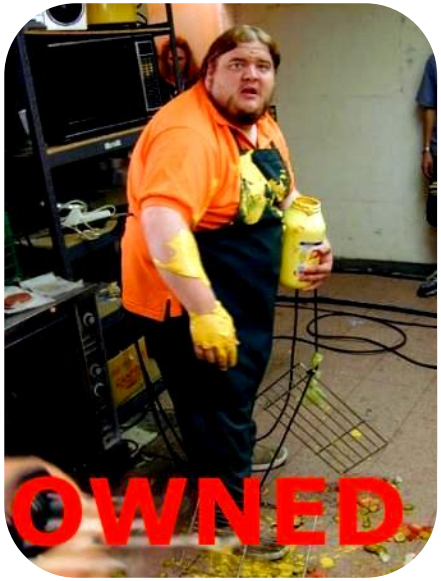
# Première confrontation (C1)

- DNS SPOOFING :
  - Requêtes interceptées :

```
dns_spoof: [google.fr] spoofed to [172.30.0.4]
dns_spoof: [www.google.fr] spoofed to [172.30.0.4]
```

OPenVPn | Shell | Shell No. 2

  - Résultat :




**Toutes les requêtes réseaux extérieurs redirigées vers notre machine : SUCCÈS !**

**Contre principal : @MAC STATIQUE**

# Première confrontation (C1)

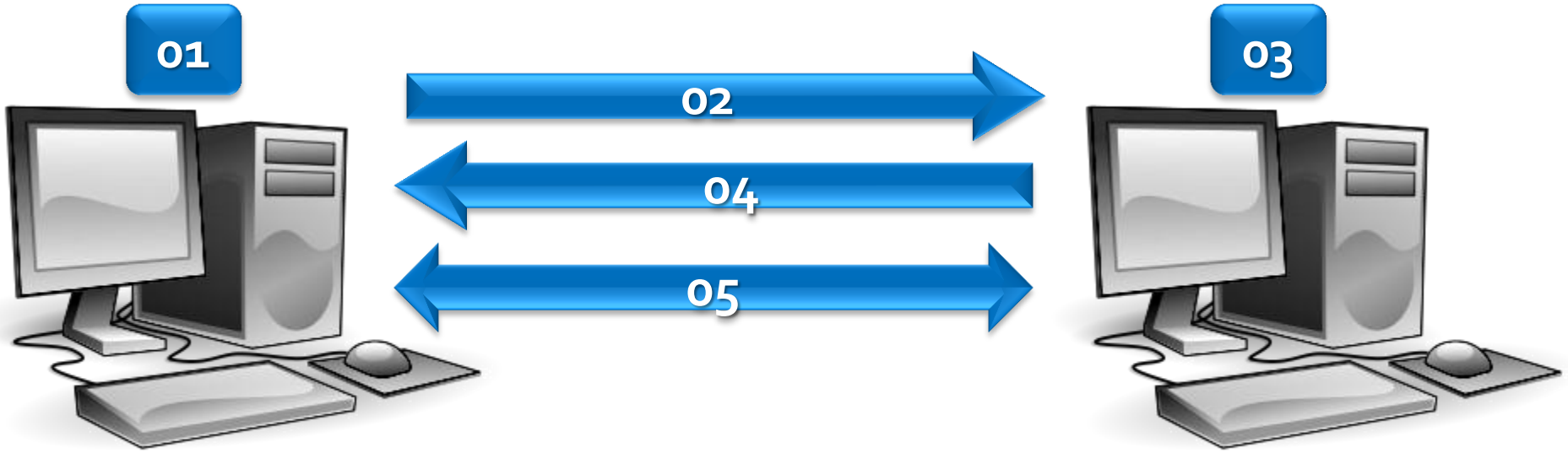
- METASPLOIT :

**« METASPLOIT est un projet OPEN-SOURCE sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. »**

**WIKI.**

# Première confrontation (C1)

- Attaque fichier .PDF malveillant :




01 **Génération PDF + mise en écoute sur port 80 via METASPLOIT**
02 **Envoi du PDF vérolé**
03 **Ouverture du PDF**
04 **Création du canal vers METASPLOIT sur le port 80**
05 **Prise de contrôle du pc cible par l'attaquant**

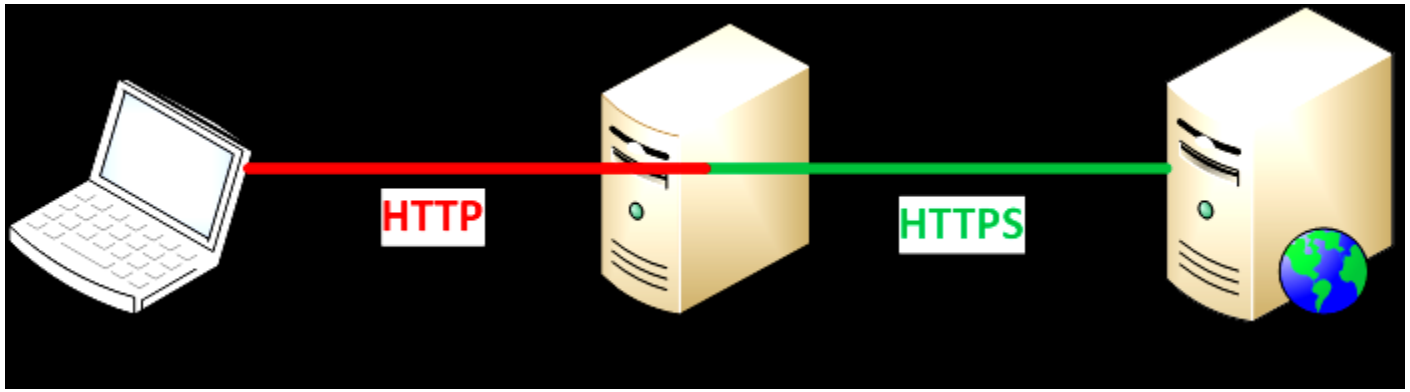
# Première confrontation (C1)

- Bilan de la C1 :
  - Première expérience **mitigée** : perte de temps, déploiements tardifs, etc…
  - Obligation d'être **réactif** et parfois **créatif** (improvisations) en fonction du déroulement de la confrontation
  - **Succès des attaques « simples »** : DNS SPOOFING en tête de liste
  - **Expérience** accumulée (confiance, découverte des confrontations, etc…)

**Mais une petite surprise nous attend…**

# C'est Noël avant l'heure !!!

- SSLSTRIP :
  - **CONSTAT** : la majorité des utilisateurs ne regardent pas l'URL affichée dans la barre de leur navigateur Web
  - **BUT** :
    - Maintenir la confiance de la victime lors de l'attaque sur sa session Web
    - Récupérer les informations dans les flux normalement en HTTPS

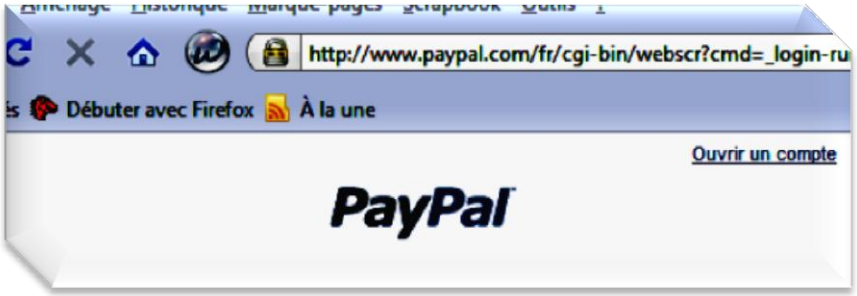



**SNIFFAGE DU TRAFIC EN CLAIR !!!**

# C'est Noël avant l'heure !!!

- SSLSTRIP :
  - Possibilité de mettre un **faux cadenas** (pas utilisé car non considéré comme crédible) :


Page Web VALIDE




Page Web PIRATÉE

# C'est Noël avant l'heure !!!

- SSLSTRIP :
  - Meilleure alternative que l'attaque SSL MiTM classique :
    - Suspicion de la victime **IMMÉDIATE**

# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage
  - **CONSTAT** :
    - Connexions multiples des utilisateurs sur leurs **WEBMAILS** et autres durant les séances de TP en salles de l'U3
    - Ordinateurs sur le même réseau de diffusion : **sniffage facilité**

Palier 01 ➔ sniffage du trafic en clair à l'aide d'ETTERCAP seulement (supporte HTTP, MSN, POP3, …)

Dangers ➔ se faire détecter par des voisins qui sont aussi victimes

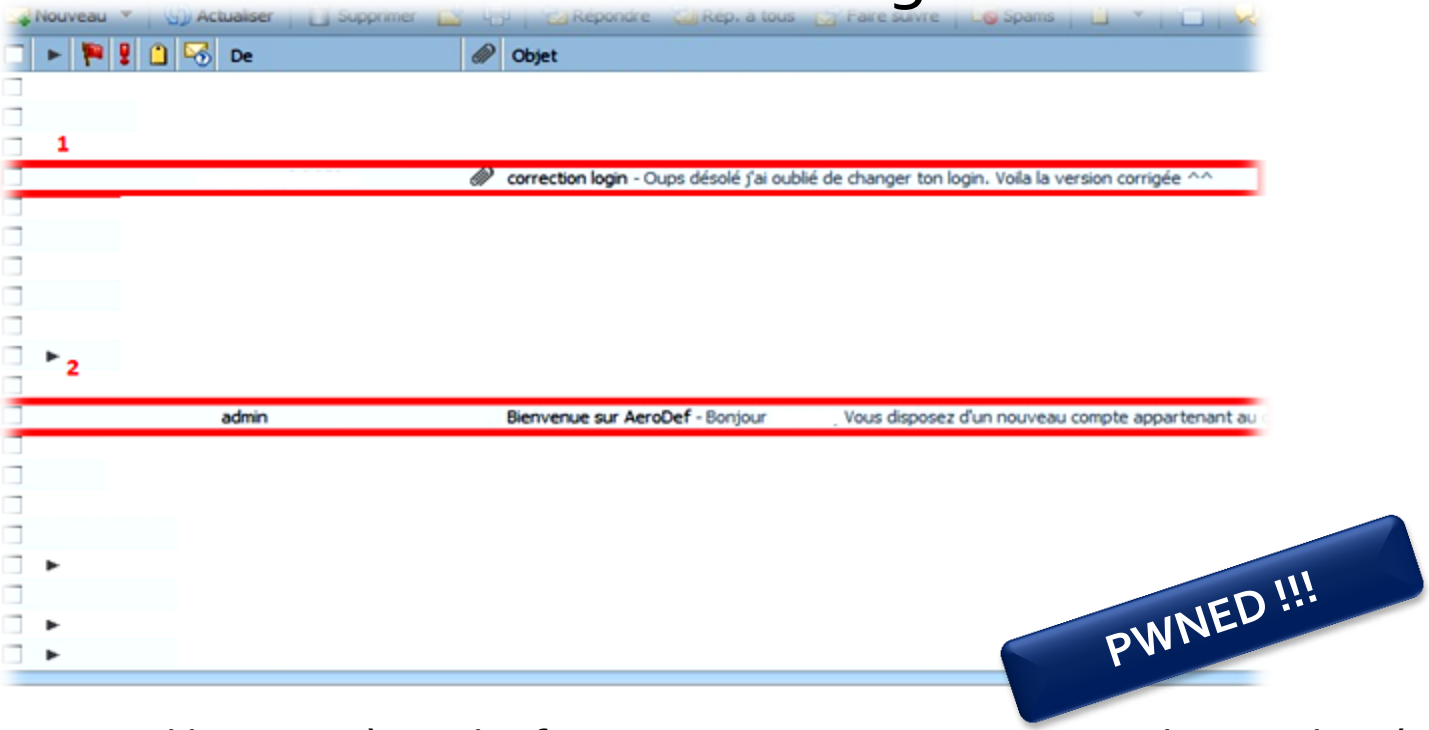
# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage
  - Peu de résultats attendus (du fait du trafic clair uniquement) mais … :
    - **HTTP : 212.27.42.91:80 -> USER: rolland.gerro@free.fr PASS: 06121988 INFO: http://zimbra.free.fr/**
  - WEBMAIL non sécurisé + utilisation d'un mot de passe simpliste :

    **POLITIQUE DE SÉCURITÉ = FAIL !!!**

# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage




1 : E-mail hors système d'informations contenant tout simplement l'intégralité des mots de passe de la machine principale Zeus de l'équipe AERODEF

2 : Récupération du mail d'accès au système d'informations AERODEF avec nom d'utilisateur, mot de passe et adresse de connexion

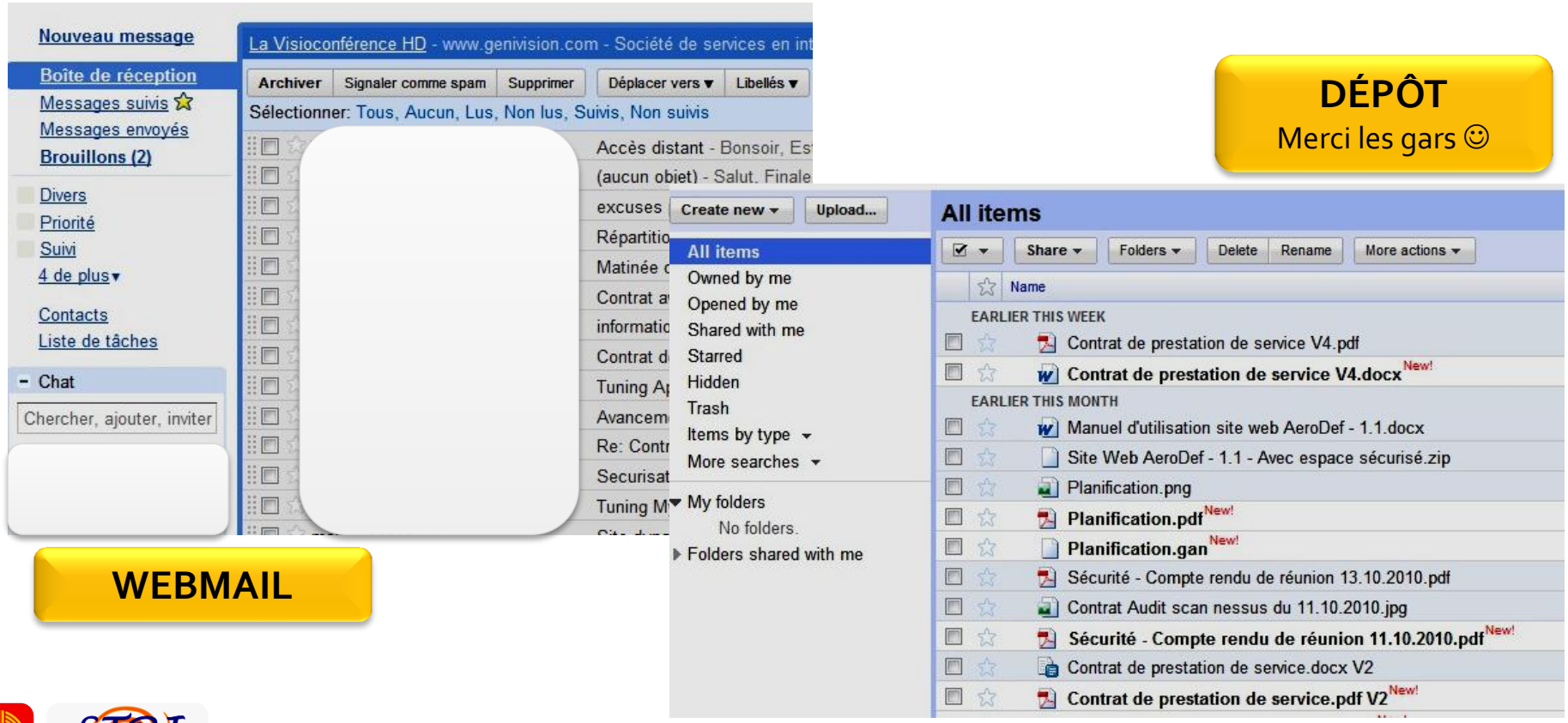
# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage
  - Remontée dans le système d'informations d'AERODEF…


**Mot de passe par défaut : NON !**
**Date de naissance : OK AGAIN !**

# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage



# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage
  - Quelques informations recueillies à ce stade du projet :
    - Intégralité des accès au serveur Zeus (SSH, SFTP,…) et machines clientes
    - Politique de sécurité
    - Comptes rendus de réunion
    - Organigramme de l'équipe AERODEF
    - Répartition des tâches
    - Contrat de prestation avec l'audit
    - Code source du site Web avec mot de passe administrateur MySQL
    - Différentes informations détaillées sur la topologie
    - Une relative assurance de la part d'AERODEF concernant leur système de communication
    - Changement des mots de passe après chaque confrontation ou événement majeur
    - Listes de tous les services opérationnels et en cours de développement ou abandonnés
    - Incapacité d'AERODEF de répondre à notre attaque DNS SPOOFING

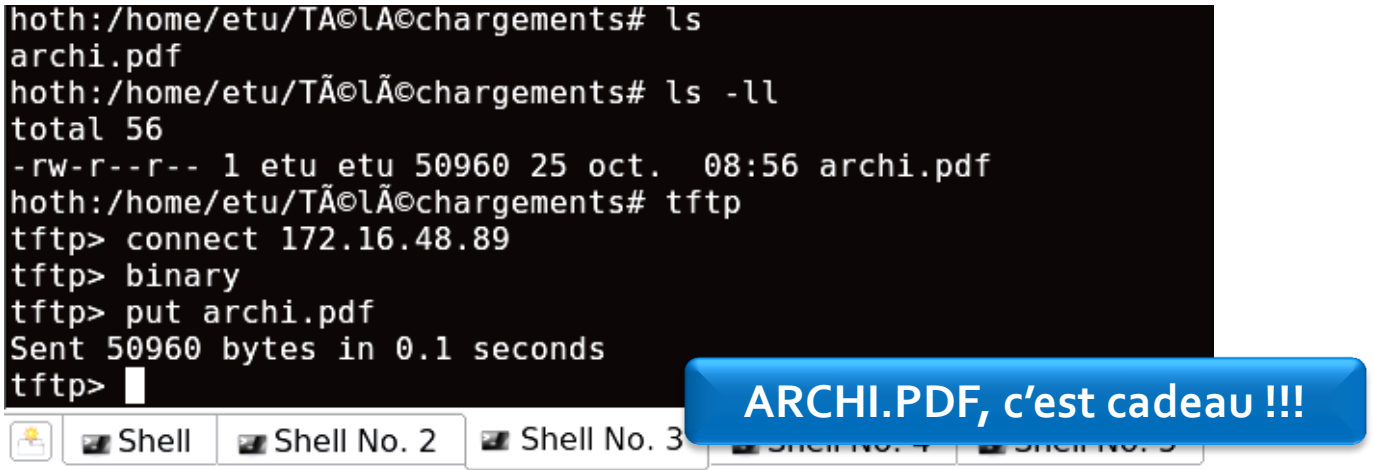
# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage
  - Tentative d'insertion de comptes utilisateurs malveillants sur le serveur Zeus lors de la nuit du 22 octobre….
    - ….mais serveur down pour cause de mauvaise manipulation d'AERODEF (merci DHClient)
  - **RÉPLIQUE** : Tentative de mise sous pression avec un bon gros e-mail acide mettant en cause la crédibilité de notre adversaire

**ERREUR** DE NOS ADVERSAIRES → **CONSÉQUENCES** SUR NOTRE ÉQUIPE

# C'est Noël avant l'heure !!!

- INFILTRATION : Phase d'atterrissage catastrophe
  - Prise de contrôle des machines clientes de la salle U2-213 lors d'une séance de TP Sécurité
  - **OBJECTIF :** Saisir toute opportunité pour la récupération d'informations via SSH



# C'est Noël avant l'heure !!!

- INFILTRATION : Phase d'atterrissage catastrophe
  - Essai d'installation de « keyloggers » logiciels à distance durant l'utilisation de la machine par la victime… ECHEC !!!
    - Erreur de manipulation : accès physique machine victime nécessaire…
  - **…interception par AERODEF en cours d'opération**

**ALARME** : Modification de tous les mots de passe !!!

# C'est Noël avant l'heure !!!

- INFILTRATION : Décollage vers la LUNE !!!
  - Retour à la case départ avec nécessité de vite réagir :
    - Apparition de SSLSTRIP en TPs (XML, JAVA, SQL, …) pour une durée totale de 5H
  - **RÉSULTAT :** récupération d'environ 60 mots de passe :
    - M2 STRI
    - Autres promotions utilisant le réseau informatique
    - Administrateurs U3

**HTTP : 66.249.92.104:80 -> USER: cyrille.lignac PASS: xxxx INFO:** http://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/?hl=fr&ui=html&zy=l&bsv=1eic6yu90

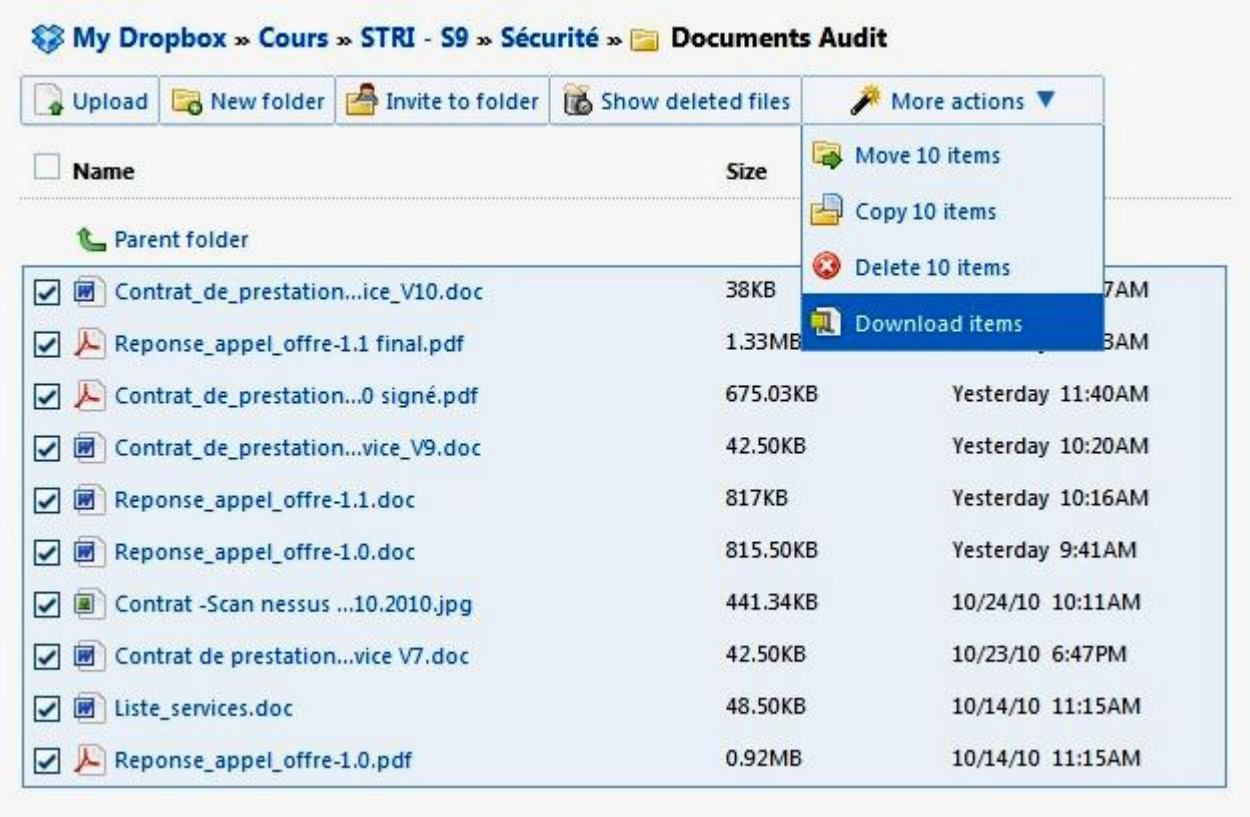
# C'est Noël avant l'heure !!!

- INFILTRATION : Décollage vers la LUNE !!!
  - Informations récupérées :
    - Fonctionnement audit : sympa IKEA_STYLE mais impénétrable !!!


  - Re-récupération documents de la défense :
    - Les derniers comptes rendus de réunion
    - Les dernières négociations avec l'audit
    - Le dernier code source du site
    - Les différentes chartes graphiques de l'entreprise
    - Les clés PGP de contact@aerodef.fr et de wanvos@gmail.com
    - Les clés et certificats du VPN M2 STRI Défense

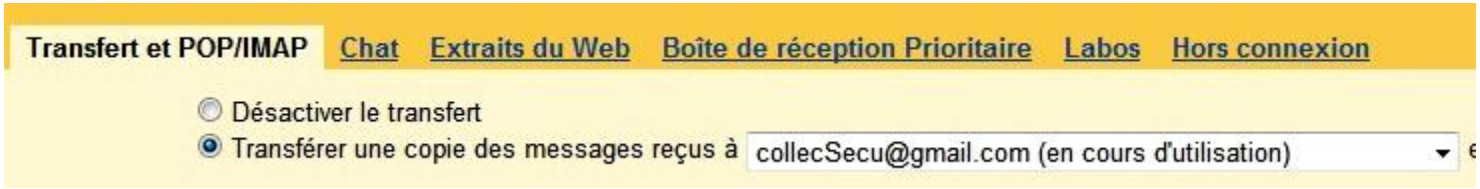
# C'est Noël avant l'heure !!!

- INFILTRATION : Décollage vers la LUNE !!!
  - Servez-vous, c'est FREE !!!



# C'est Noël avant l'heure !!!

- INFILTRATION : Décollage vers la LUNE !!!
  - Transfert des e-mails :




  - …mais toujours pas de mots de passe concernant les équipements !!!

# C'est Noël avant l'heure !!!

- INFILTRATION : On a marché sur la LUNE !!!
  - **OBJECTIFS :** se servir de tous les comptes e-mails pour imaginer un scénario permettant de tromper la défense et de récupérer les accès à leur architecture
  - **CONTEXTE :** se servir du long week-end de fin octobre pour éviter tout contact réel pouvant compromettre notre attaque
  - **OUTILS :** potentiellement toutes les adresses e-mail à notre disposition et surtout les règles de filtrage de GMAIL
  - Choix de l'utilisation du mail de Jacques MARTIN car nous avions détecté un problème de mot de passe à l'origine d'AERODEF

**REJOUER CE SCÉNARIO DE BASE = PLUS CRÉDIBLE**

**ETAPE 1**

- Jacques Martin(jacques-martin@gmail.com) vers admin@aerodef.fr, jeremie.dupont@gmail.com, thierry@henry.fr
- **Sujet :** Problème connexion au compte AERODEF, demande d'un nouveau mot de passe
- **Objectif Attaque** : Infiltrer le SI AERODEF

**ETAPE 2**

- thierry@henry.fr vers Administrateur AERODEF (thierry.luron@aerodef.fr), jeremie.dupont@gmail.com
- **Sujet :** Suspicion d'attaque, vérification de l'identité de l'émetteur initial
- **Risque de détection de l'attaque !!!**

**ETAPE 3**

- jeremie.dupont@gmail.com vers thierry.luron@aerodef.fr
- **Sujet :** Vérification de l'identité de l'émetteur initial
- **Objectif :** Court-circuiter le membre suspicieux pour accréditer l'attaque

**ETAPE 3**

- jeremie.dupont@gmail.com vers thierry.luron@aerodef.fr
- **Sujet :** Vérification de l'identité de l'émetteur initial
- **Objectif :** Court-circuiter le membre suspicieux pour accréditer l'attaque

**ETAPE 4**

- admin@aerodef.fr vers jacques-martin@gmail.com
- **Sujet :** Envoi nouveau mot de passe

**ETAPE 5**

- jacques-martin@gmail.com vers admin@aerodef.fr
- **Sujet :** Problème login (réel cette fois ci)

**ETAPE 6**

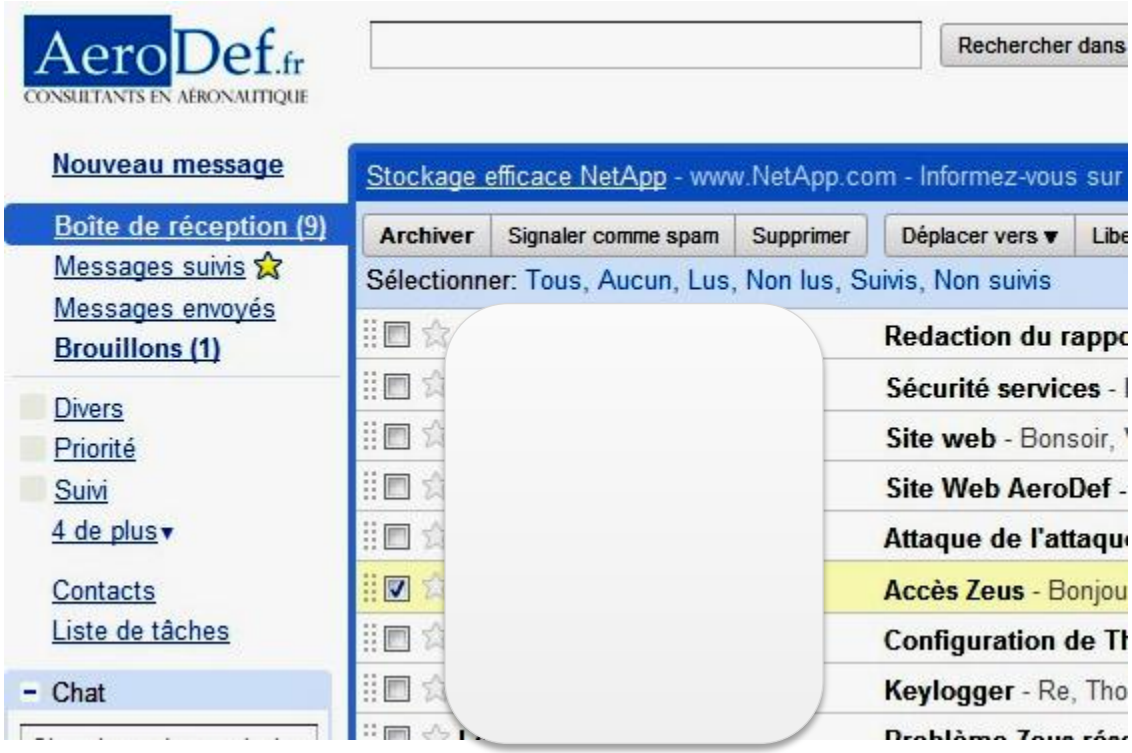
- admin@aerodef.fr vers jacques-martin@gmail.com
- **Sujet :** Explication connexion (utilisation nom.prenom@aerodef.fr au lieu de prenom.nom@aerodef.fr**)**
- **Attaque : SUCCES**

**ETAPE 7**

- **Suppression** de toutes les traces sur les boites e-mails compromises et écriture d'un faux mail d'admin@aerodef.fr pour justifier d'un changement de mot de passe pour raisons de sécurité

# C'est Noël avant l'heure !!!

- INFILTRATION : On a marché sur la LUNE !!!
  - **WE ARE BACK YEAH !!!**



# C'est Noël avant l'heure !!!

- INFILTRATION : On a marché sur la LUNE !!!
  - Récupération inventaire machines :

| | | | |
|---|---|---|---|
| | | | 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 |

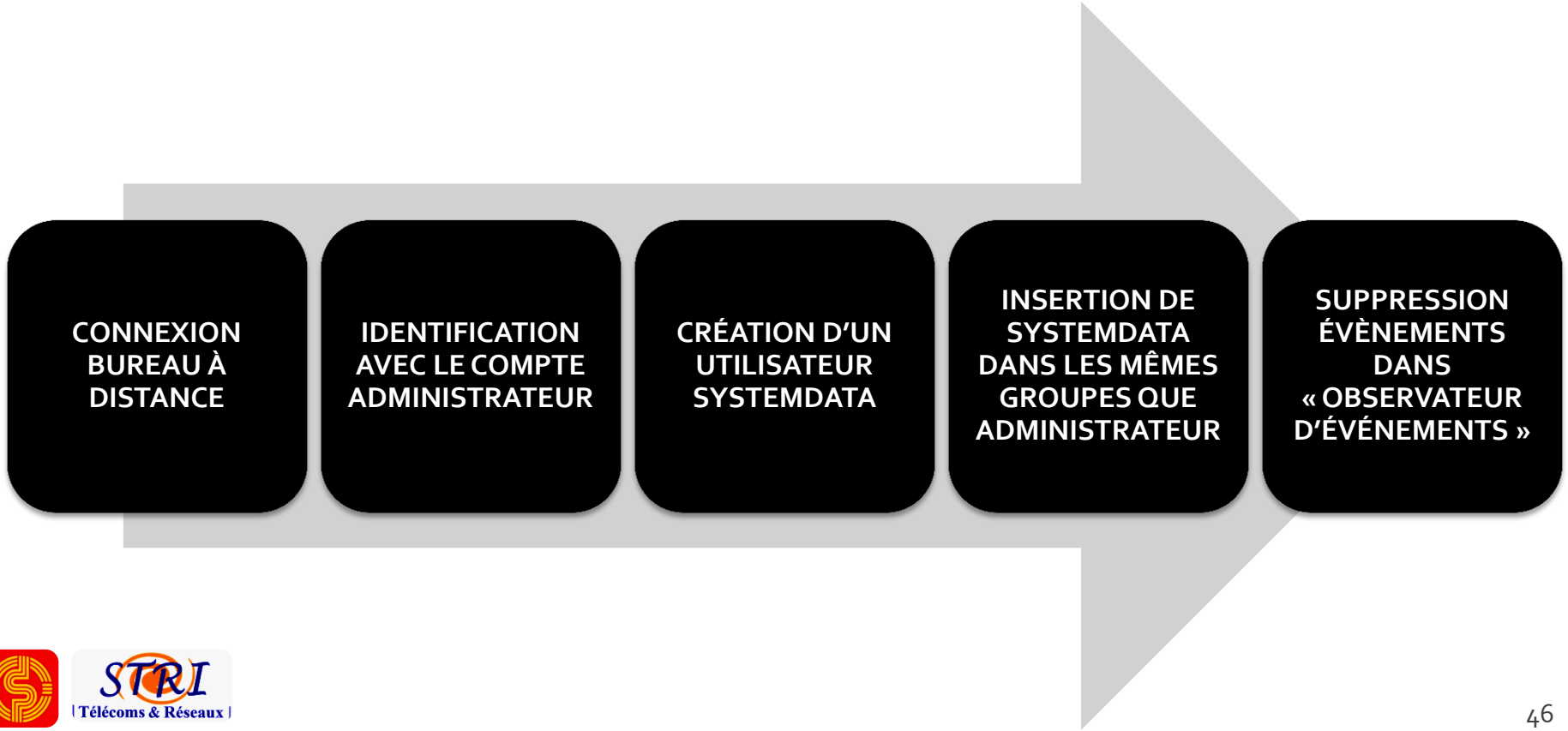
    - Récupération des documents suivants :
      - Intégralité mots de passe (serveur Zeus + contrôleur de domaines) malgré le chiffrage
      - Dernières informations (dont raison du changement de mot de passe)…
      - …mais moins d'informations auxiliaires qu'auparavant du fait du non-statut de chef d'équipe

# C'est Noël avant l'heure !!!

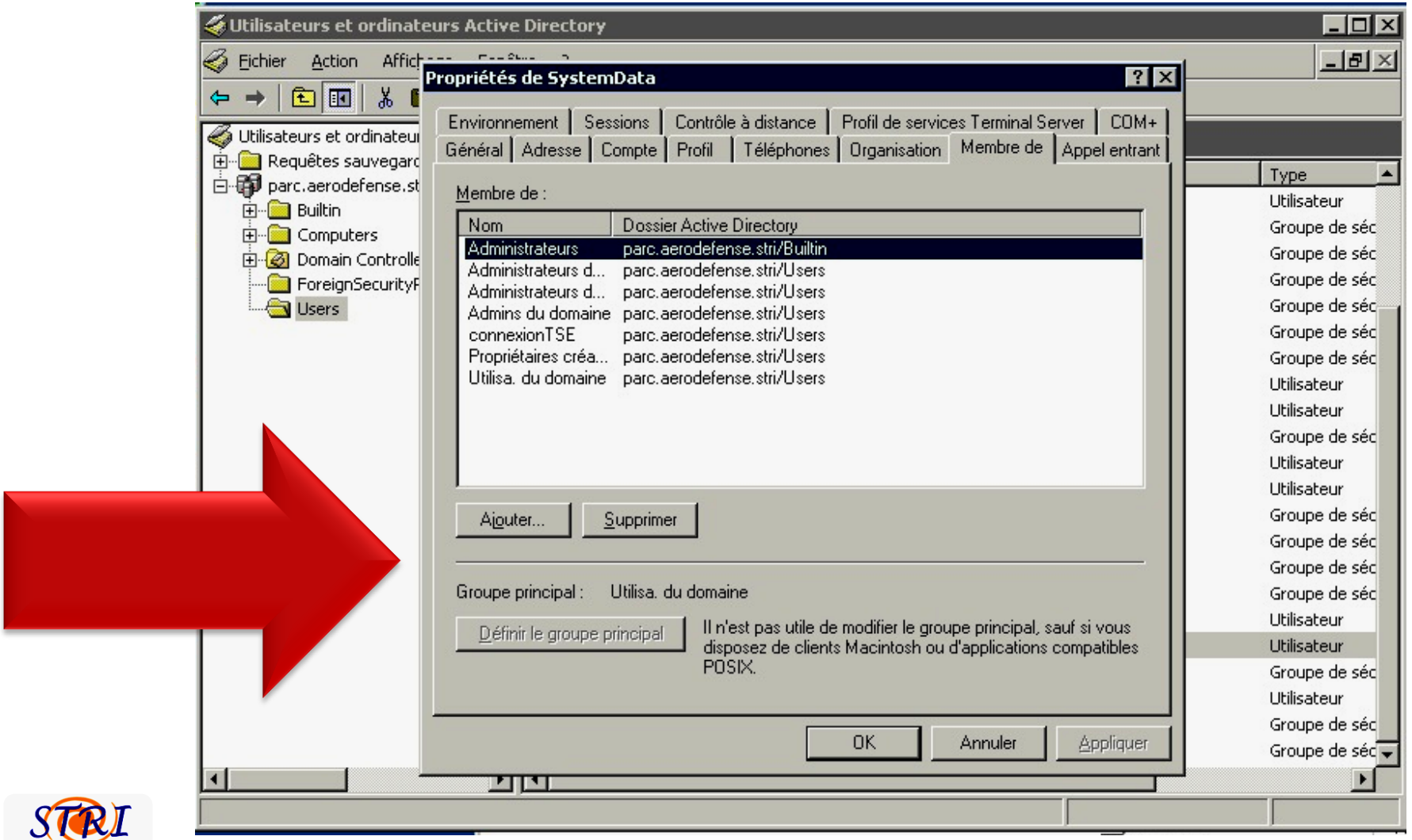
- INFILTRATION : On a marché sur la LUNE !!!
  - Anticipation sur tout changement de mots de passe :
    - **Adresses de transfert déjà en place**
    - Utilisateurs malicieux sur les serveurs pour prise de contrôle lors de la 3ème confrontation ➔ **À FAIRE**
    - **OBJECTIF FINAL :** faire autant partie d'AERODEF qu'un autre membre d'AERODEF (voire plus… ☺)

# C'est Noël avant l'heure !!!

- INFILTRATION : On a marché sur la LUNE !!!
  - Infiltration dans le contrôleur de domaine :

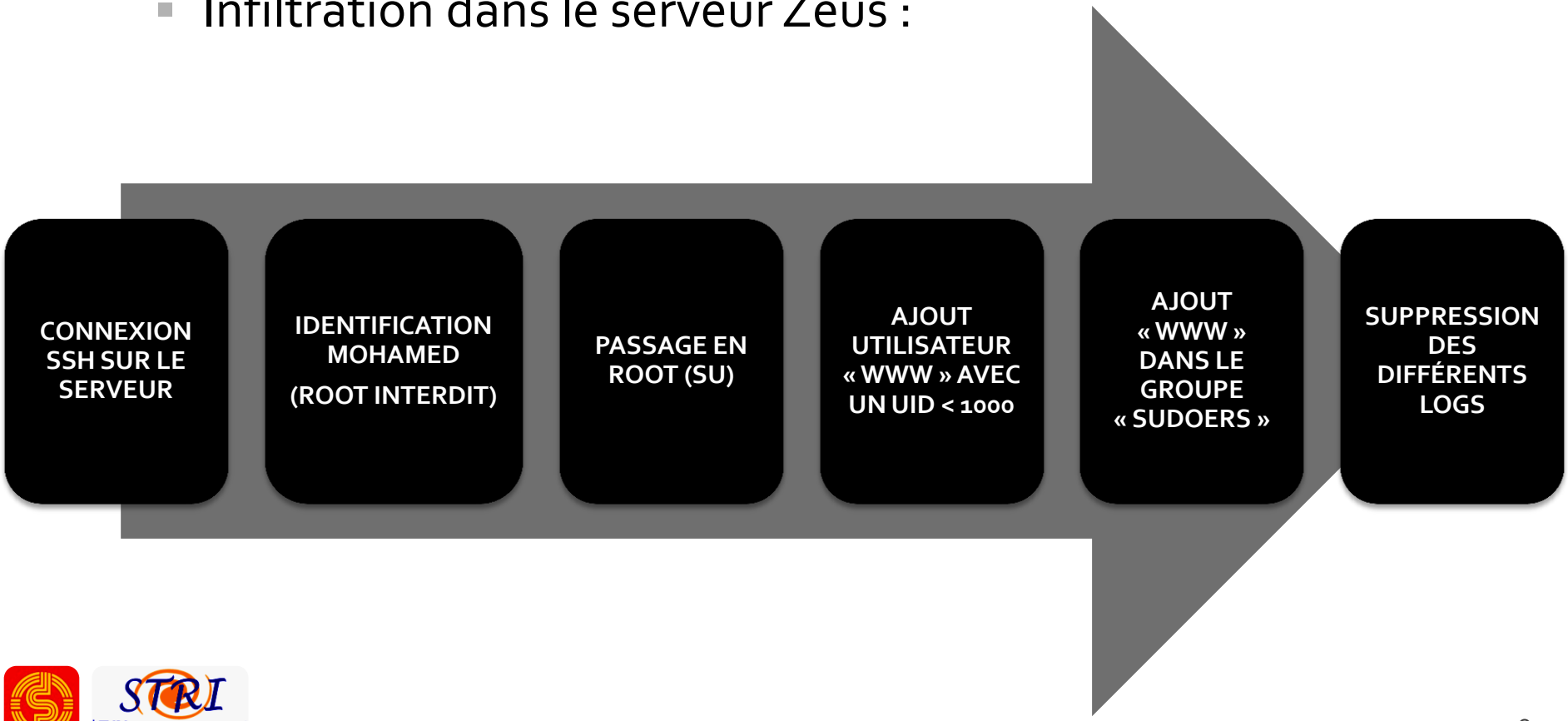


# C'est Noël avant l'heure !!!



# C'est Noël avant l'heure !!!

- INFILTRATION : On a marché sur la LUNE !!!
  - Infiltration dans le serveur Zeus :



# C'est Noël avant l'heure !!!

- Parades à SSLSTRIP :
  - HSTS (HTTP Strict Transport Security)
    - Permettre de forcer la connexion d'un site web en HTTPS et ainsi de se protéger d'une attaque type « Man in the Middle »

~~SSLSTRIP~~

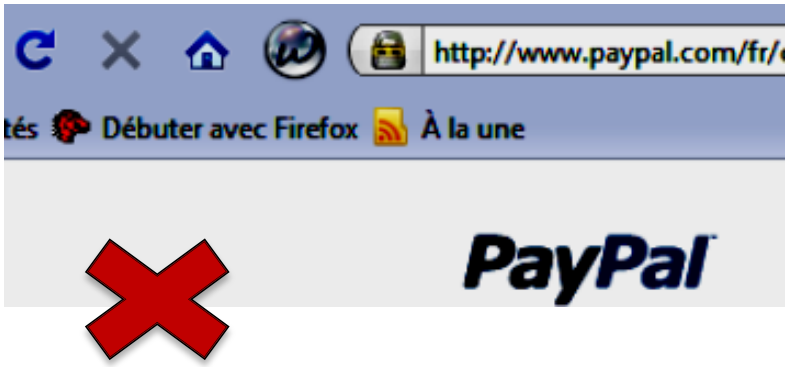
    - Idée pensée par 2 chercheurs C. JACKSON et A. BARTH (Université de STANDFORD) avec ForceHTTPS
    - Spécification IETF : http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02 (statut = « STANDARD TRACK »)

# C'est Noël avant l'heure !!!

- Parades à SSLSTRIP : **HSTS**
  - Principe : forcer le chiffrement des données via l'entête HTTP.
  - Exemple sous Apache :
    - **Header set Strict-Transport-Security "max-age=500"**
    - **Header append Strict-Transport-Security includeSubDomains**
  - Faille : requête initiale sans protection
    - Nécessité du navigateur de posséder une liste pré-chargée
  - Navigateurs supportant HSTS :
    - GOOGLE Chrome (version 4 – sortie aout 2009)
    - MOZILLA Firefox (version 4 – sortie prévu fin 2010)
    - Non prévu dans Internet Explorer 9, la future version du navigateur utilisé dans les salles de TP du bâtiment U2…

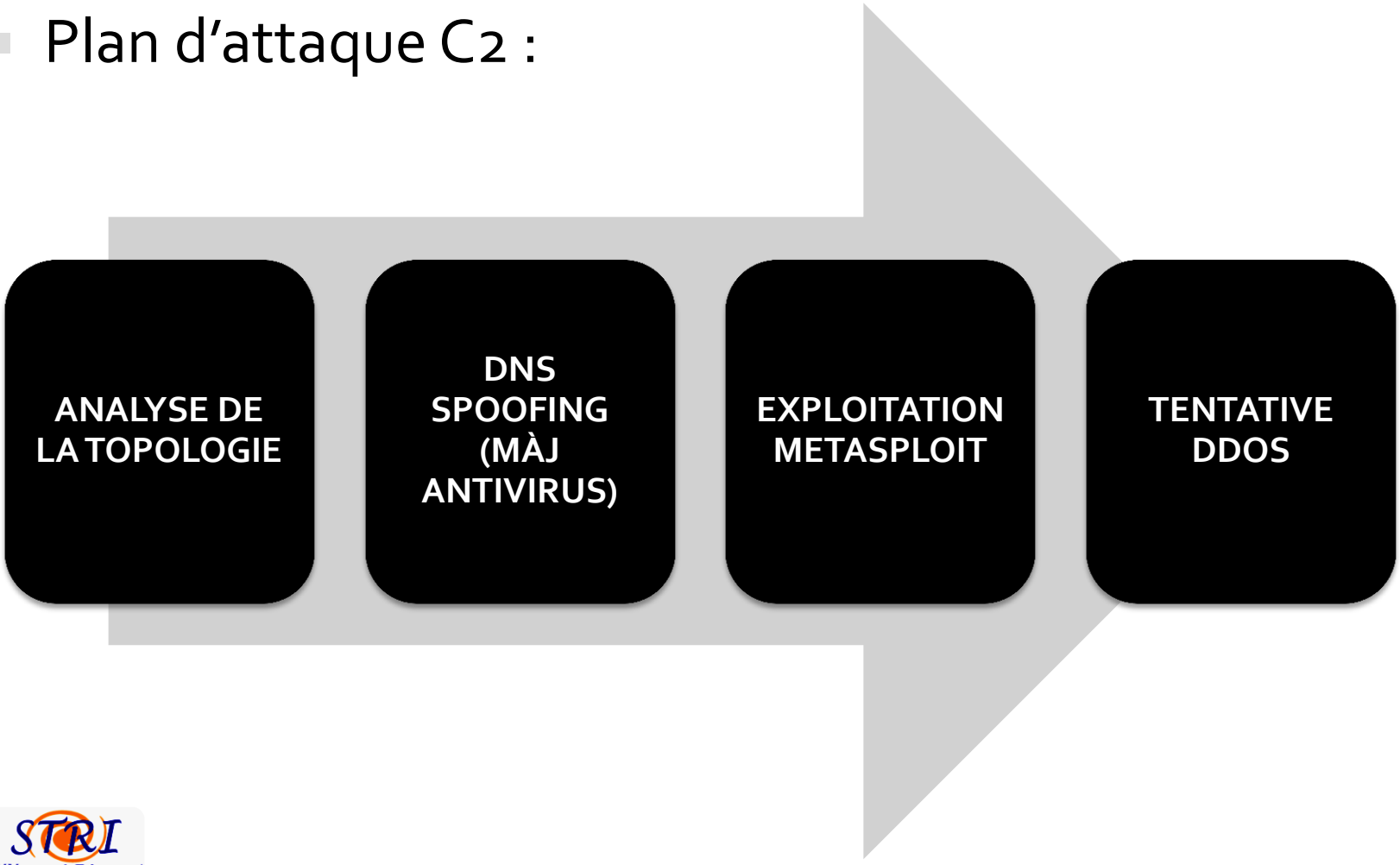
# C'est Noël avant l'heure !!!

- Parades à SSLSTRIP : **Interface CLAVIER/CHAISE**
  - Vérifier l'utilisation d'HTTPS par son navigateur :




# Deuxième confrontation (C2)

- Plan d'attaque C2 :



# Deuxième confrontation (C2)

- La communication :
  - Aucun réel changement au niveau INTERNE
  - **Nouveaux problèmes** rencontrés par l'équipe de défense : perte de temps, tensions, etc…

**Aucun bluff de l'équipe défense (cf. C1)**

  - **Responsable de communication sollicité** : calmer le jeu, organiser avec les autres responsables, etc…
  - Prise de conscience de l'importance d'assurer une communication satisfaisante : fond **et** forme

# Deuxième confrontation (C2)

- METASPLOIT : **Exploit n°1 : CVE-2010-1818**

http://www.metasploit.com/modules/exploit/windows/browser/apple_quicktime_marshaled_punk

À la une

Etat du site

### Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution

This module exploits a memory trust issue in Apple QuickTime 7.6.7. When processing a specially-crafted HTML page, the QuickTime ActiveX control will treat a supplied parameter as a trusted pointer. It will then use it as a COM-type pUnknown and lead to arbitrary code execution. This exploit utilizes a combination of heap spraying and the QuickTimeAuthoring.qtx module to bypass DEP and ASLR. This module does not opt-in to ASLR. As such, this module should be reliable on all Windows versions. NOTE: The addresses may need to be adjusted for older versions of QuickTime.

**Rank**

- Great

**Authors**

- Ruben Santamarta < >
- jduck < jduck [at] metasploit.com >

**References**

- CVE-2010-1818
- OSVDB-67705
- http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1

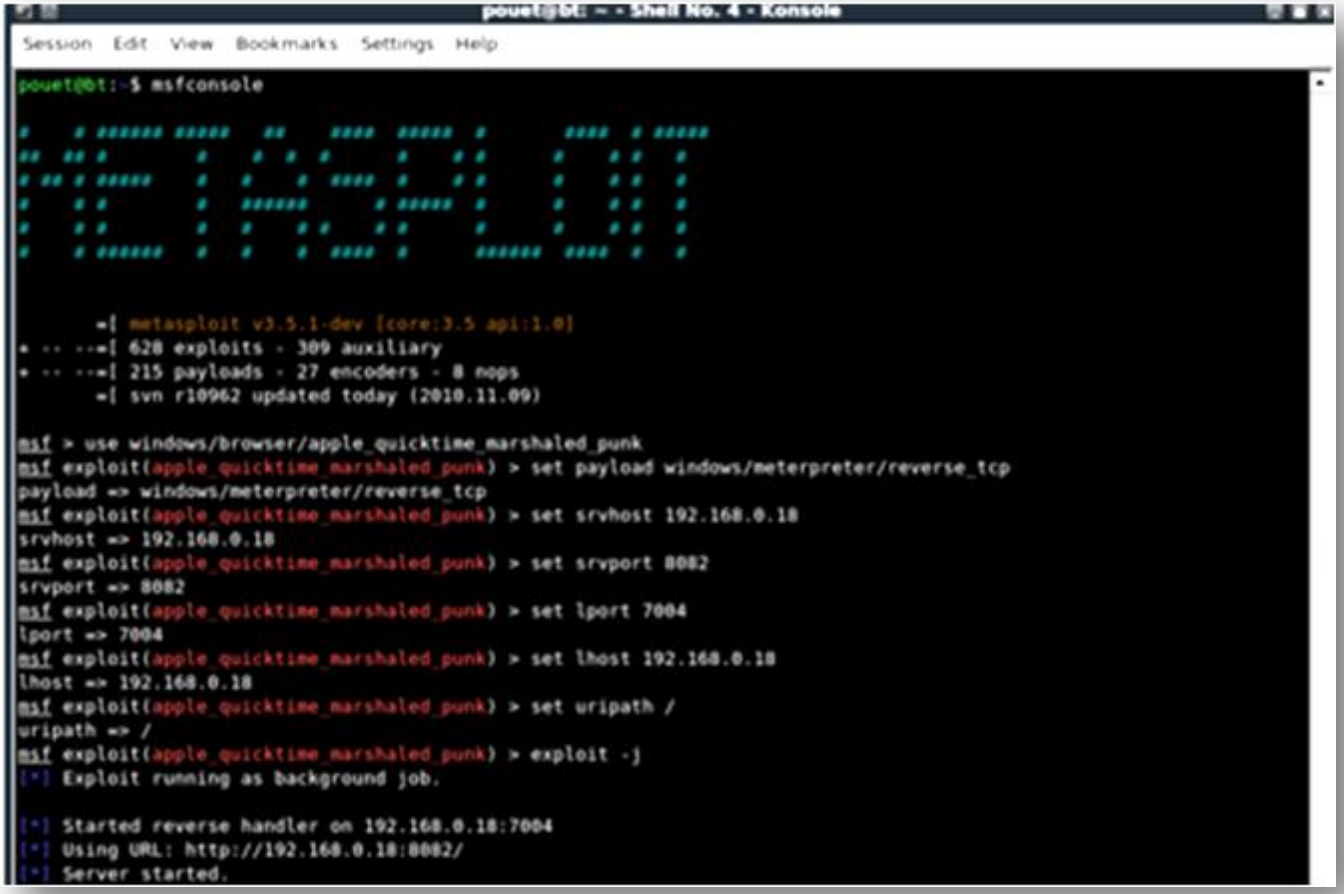
**Exploit Targets**

- 0 - Apple QuickTime Player 7.6.6 and 7.6.7 on Windows XP SP3 (default)

STRI Télécoms & Réseaux

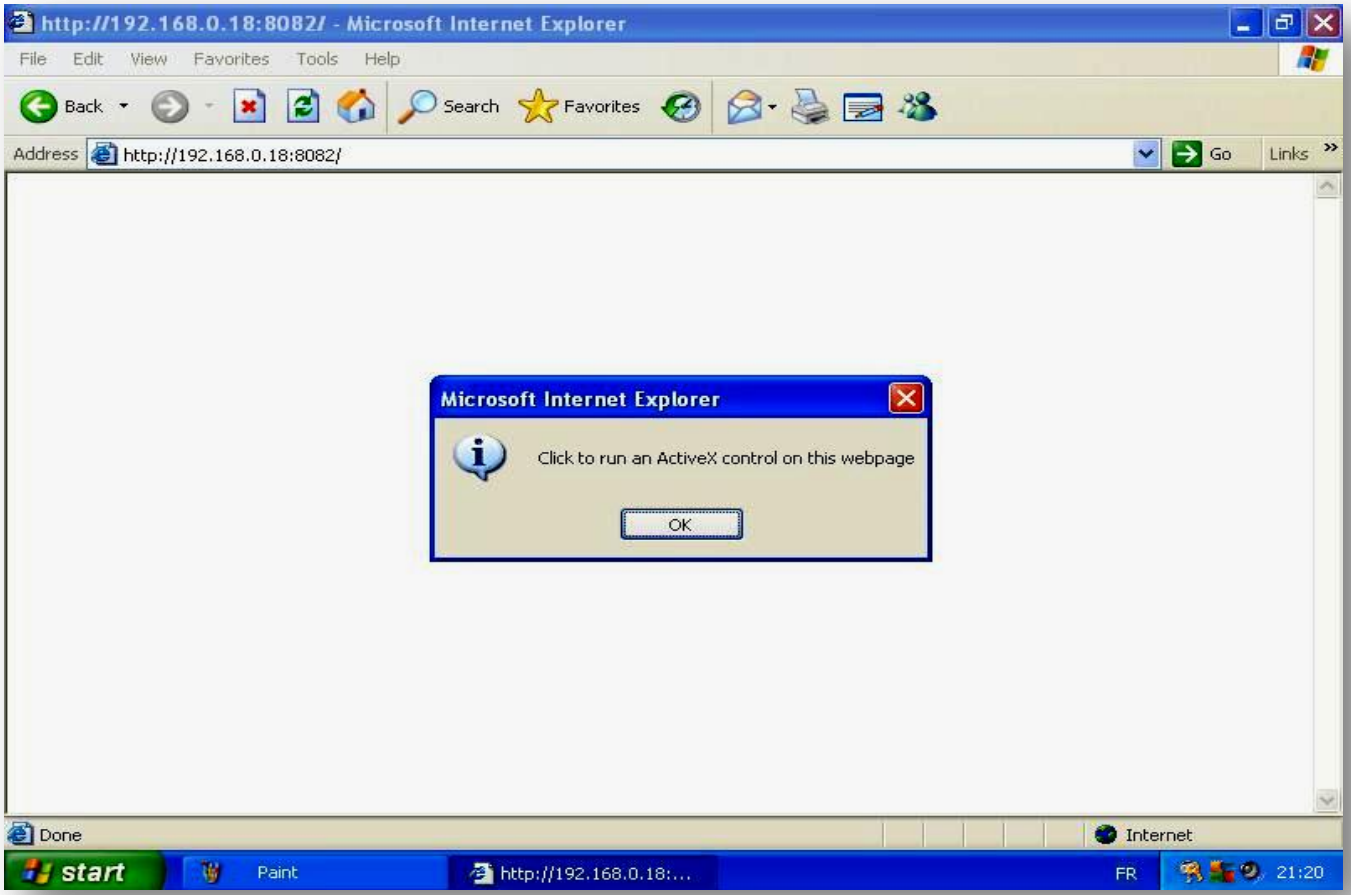
# Deuxième confrontation (C2)

- METASPLOIT : **CFG et LANCEMENT**



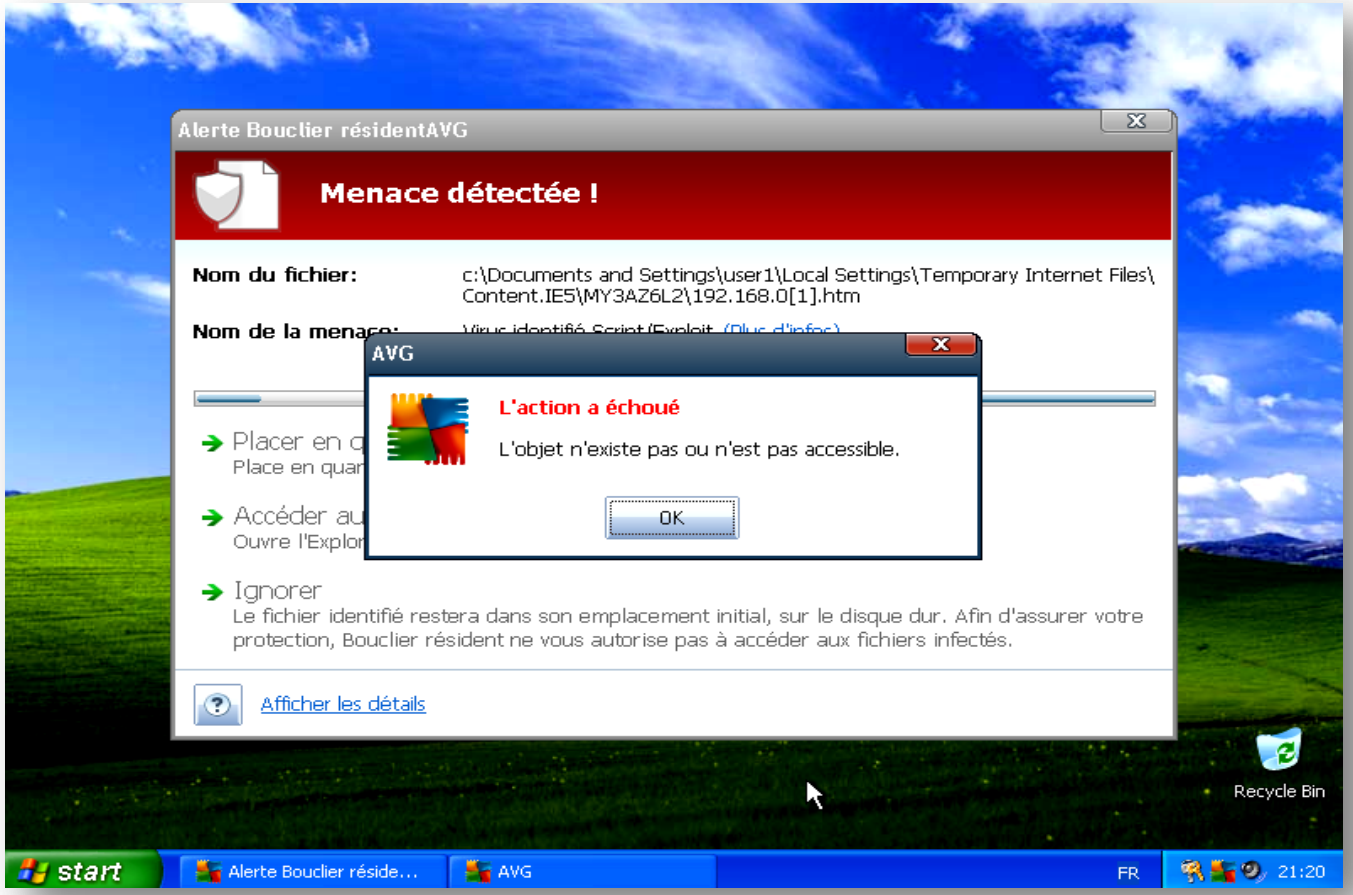
# Deuxième confrontation (C2)

- METASPLOIT : **CÔTÉ VICTIME…**



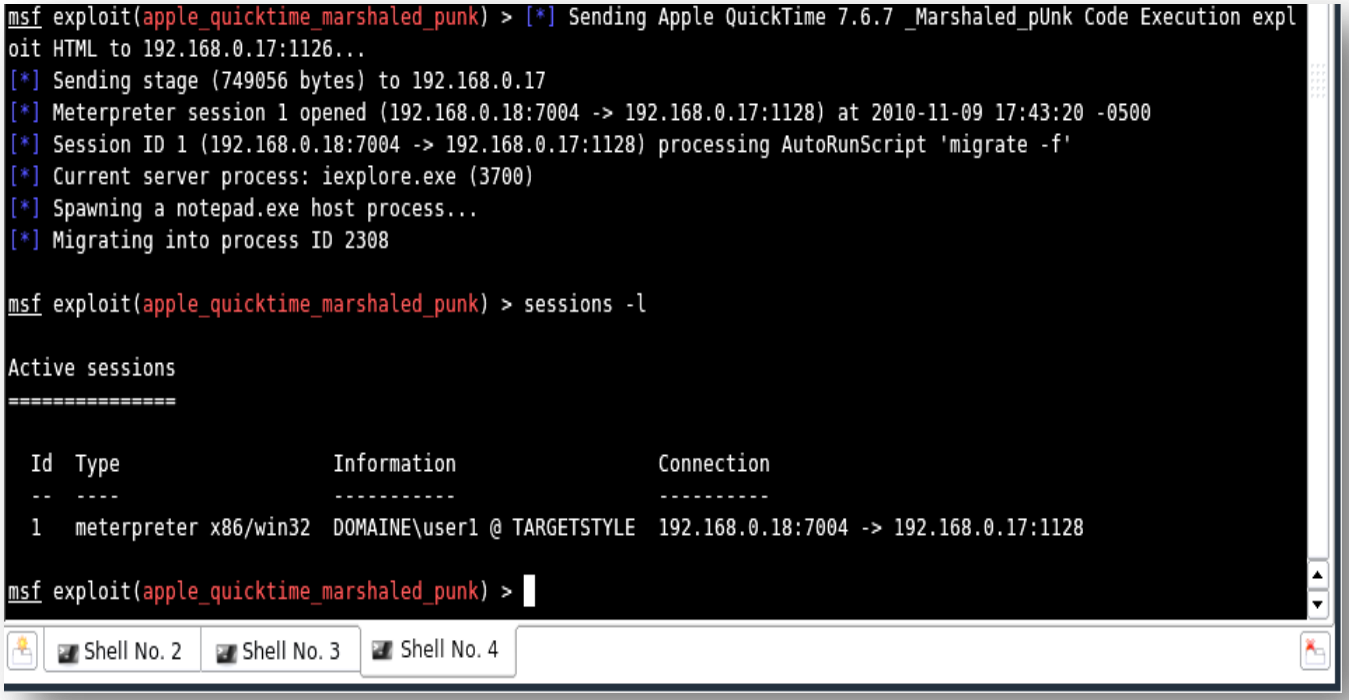
# Deuxième confrontation (C2)

- METASPLOIT : ☺



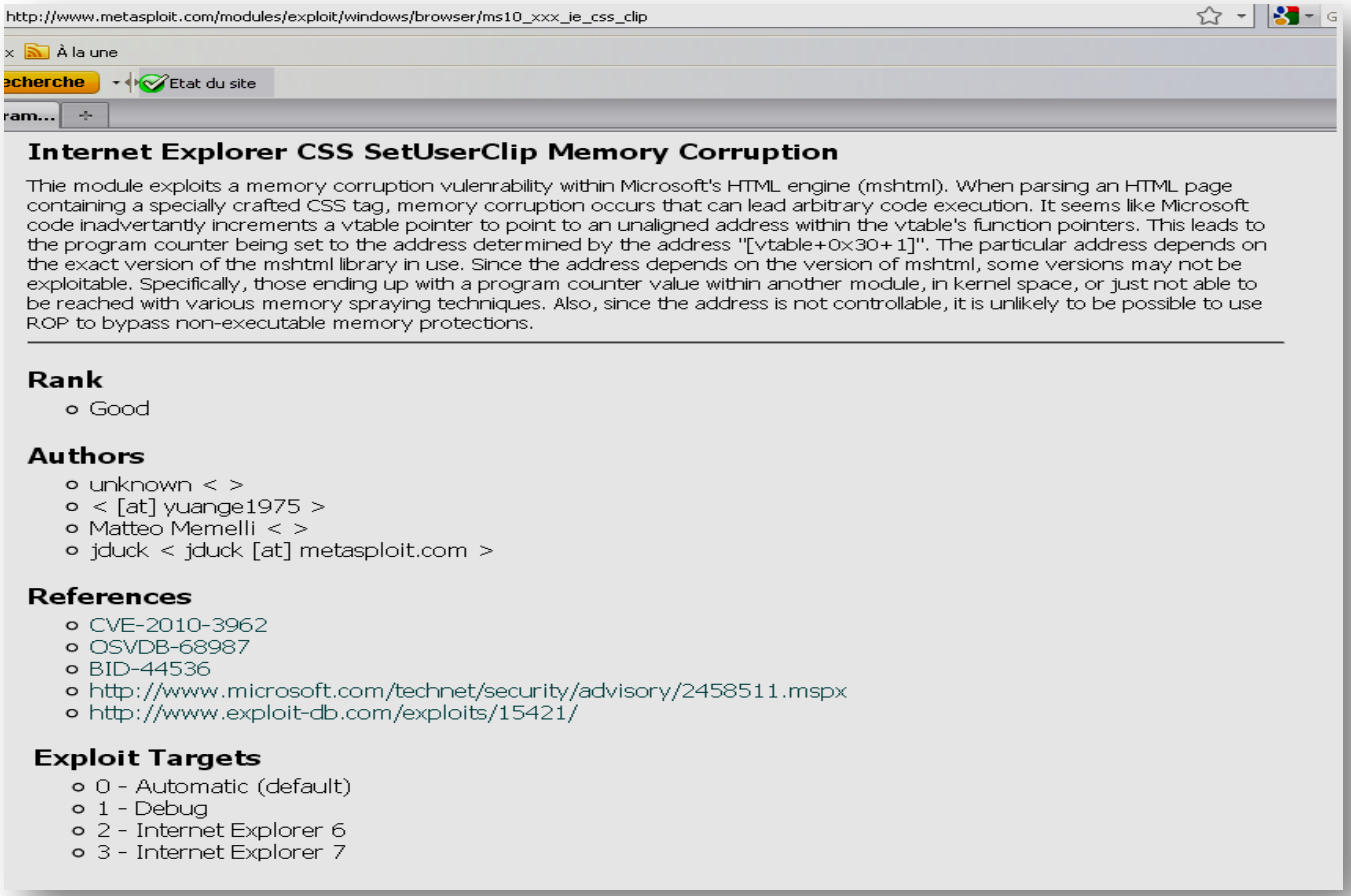
# Deuxième confrontation (C2)

- METASPLOIT : **GAME OVER !!!**



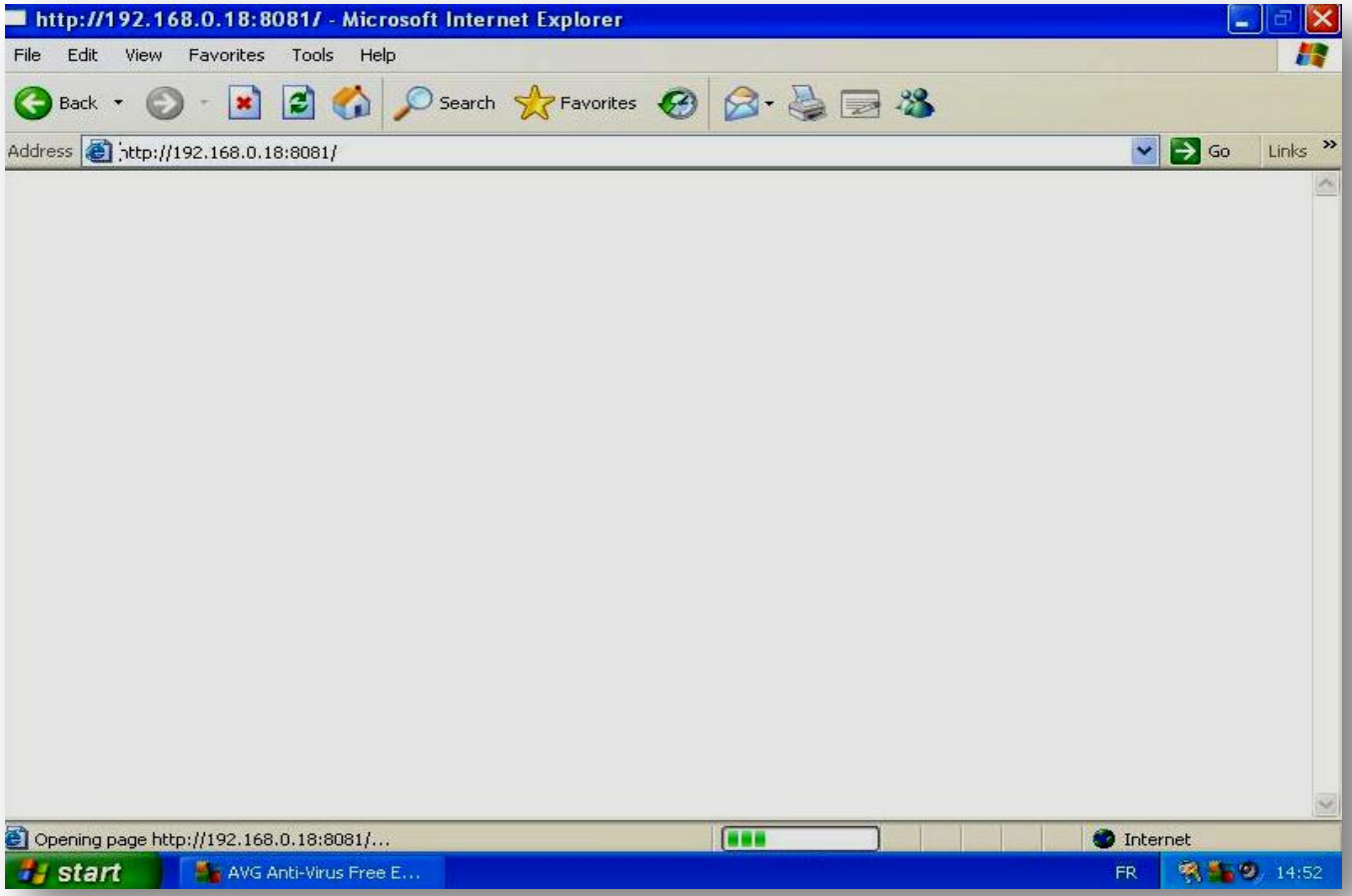
# Deuxième confrontation (C2)

- METASPLOIT : **Exploit n°2 : CVE-2010-3962 [oday]**



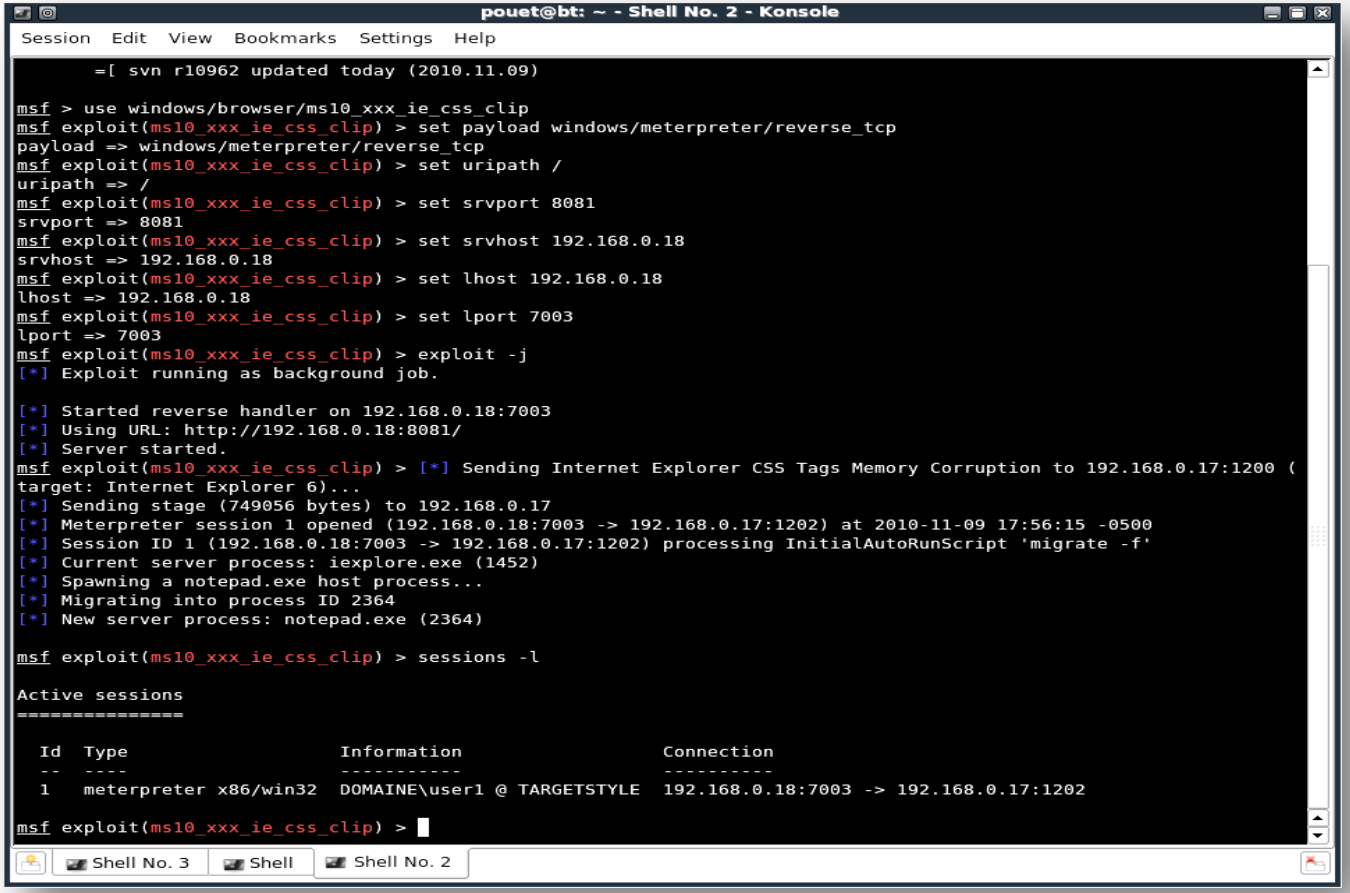
# Deuxième confrontation (C2)

- METASPLOIT : **BYPASS**



# Deuxième confrontation (C2)

- METASPLOIT : **PWNED !!!**



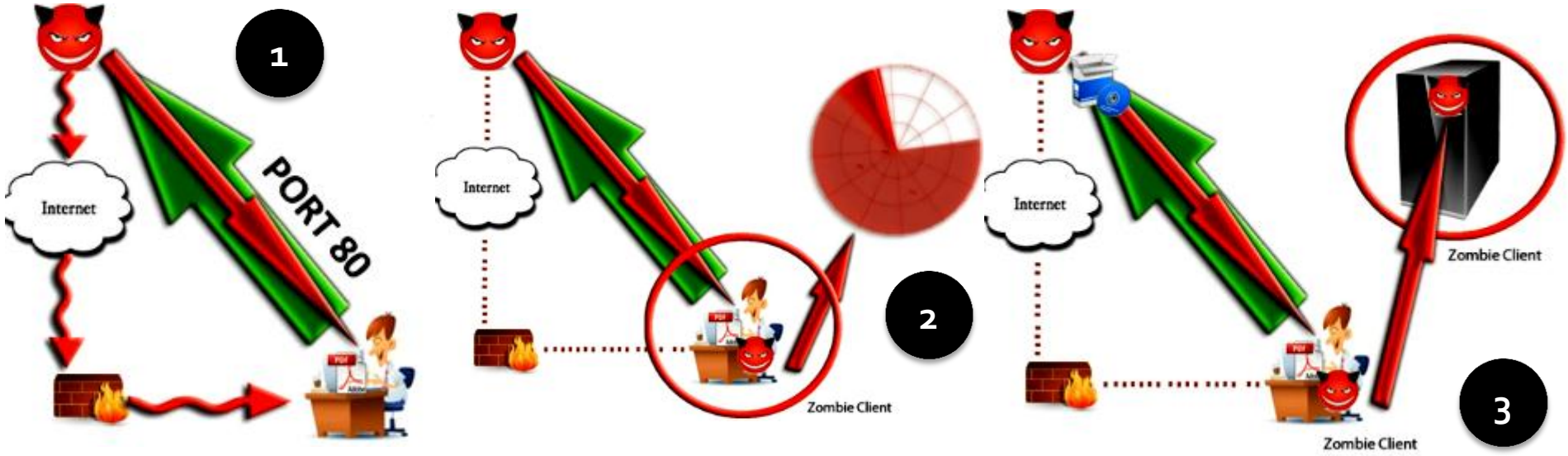
# Deuxième confrontation (C2)

- METASPLOIT : **Accès persistant et KILL-AVG**
  - 1 | Générer une Backdoor exécutable & lancer listenner
  - 2| Upload de la Backdoor vers le dossier Démarrage de Windows
  - 3| Supprimer clé RUN du registre
    *[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]*
  - 4 | Redémarrage de la machine
  - 5 | Suppression de l'exécutable « avg.exe »
  - 6 | Welcome Home !

# Deuxième confrontation (C2)

- METASPLOIT : **Méthode du pivot**

**S'introduire en profondeur dans un réseau privé depuis chez soi café en main**



# Deuxième confrontation (C2)

- **INJECTION SQL :**

**Avoir un accès administrateur sur le site**

**Modifier les news du site**

# Deuxième confrontation (C2)

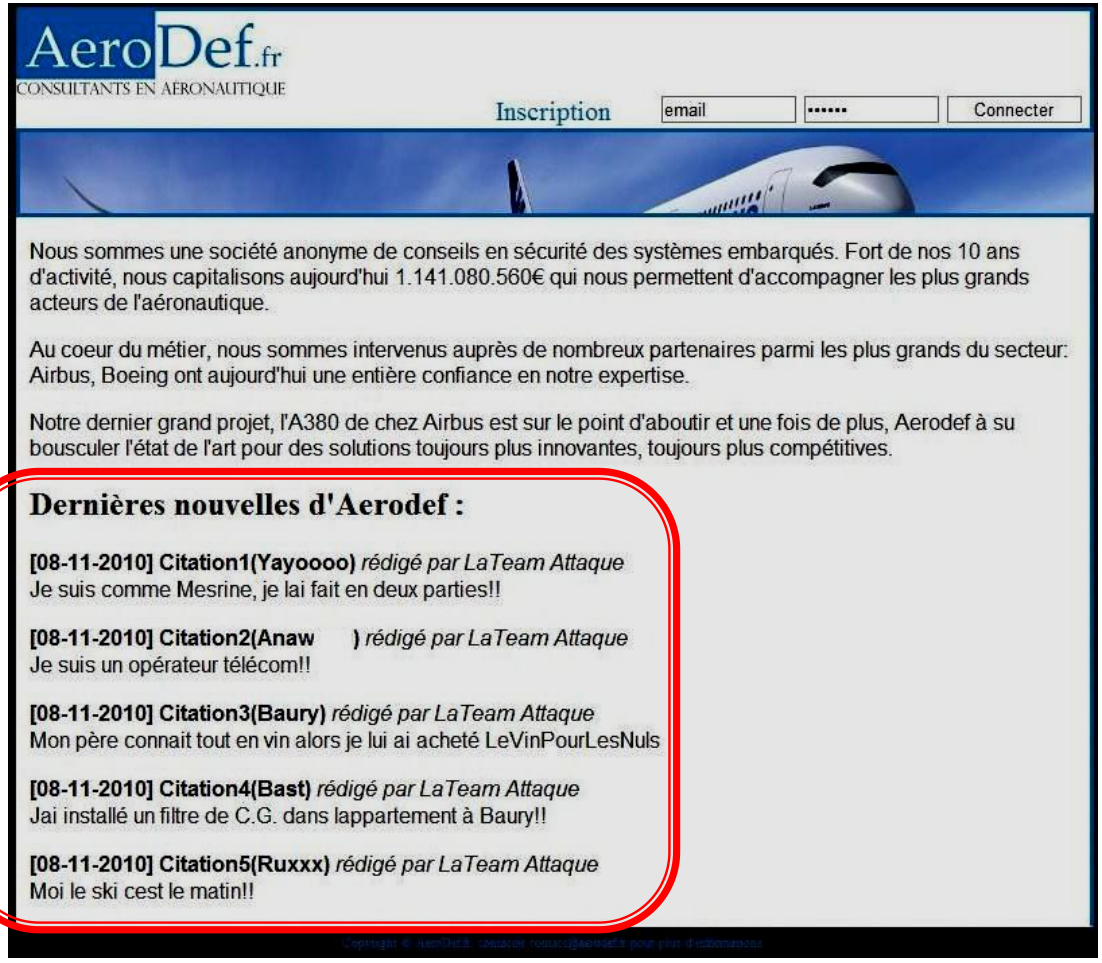
- **INJECTION SQL :**

**CRÉATION D'UN COMPTE « ADMIN »**

# Deuxième confrontation (C2)

- **INJECTION SQL :**

**INSERTION DE NOUVELLES**




STRI
Télécoms & Réseaux

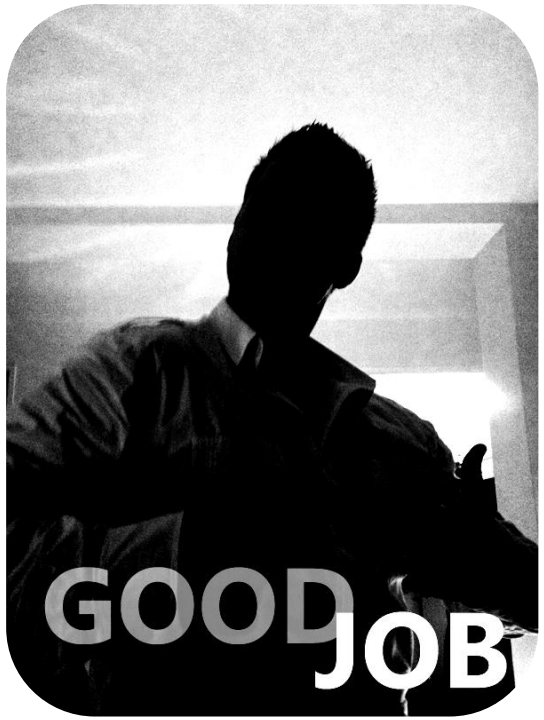
# Deuxième confrontation (C2)

- **INJECTION SQL :**

DIFFICULTÉS → Changement mot de passe BDD

→ Changement structure table SQL

→ Protection code malveillant



# Deuxième confrontation (C2)

**Script de DDoS :**

```
#!/bin/bash
i=0
while ((i < 1))
do
a=$[ ( $RANDOM % 255 ) ]
b=$[ ( $RANDOM % 255 ) ]
c=$[ ( $RANDOM % 255 ) ]
d=$[ ( $RANDOM % 255 ) ]
nmap 172.30.0.3,5 -O --data-length 1400 -S $a.$b.$c.$d -e
eth0 –min-parallelism 100 >/dev/null 2>/dev/null
done
```

…mais aucun résultat intéressant…filtrage de Cooper ?

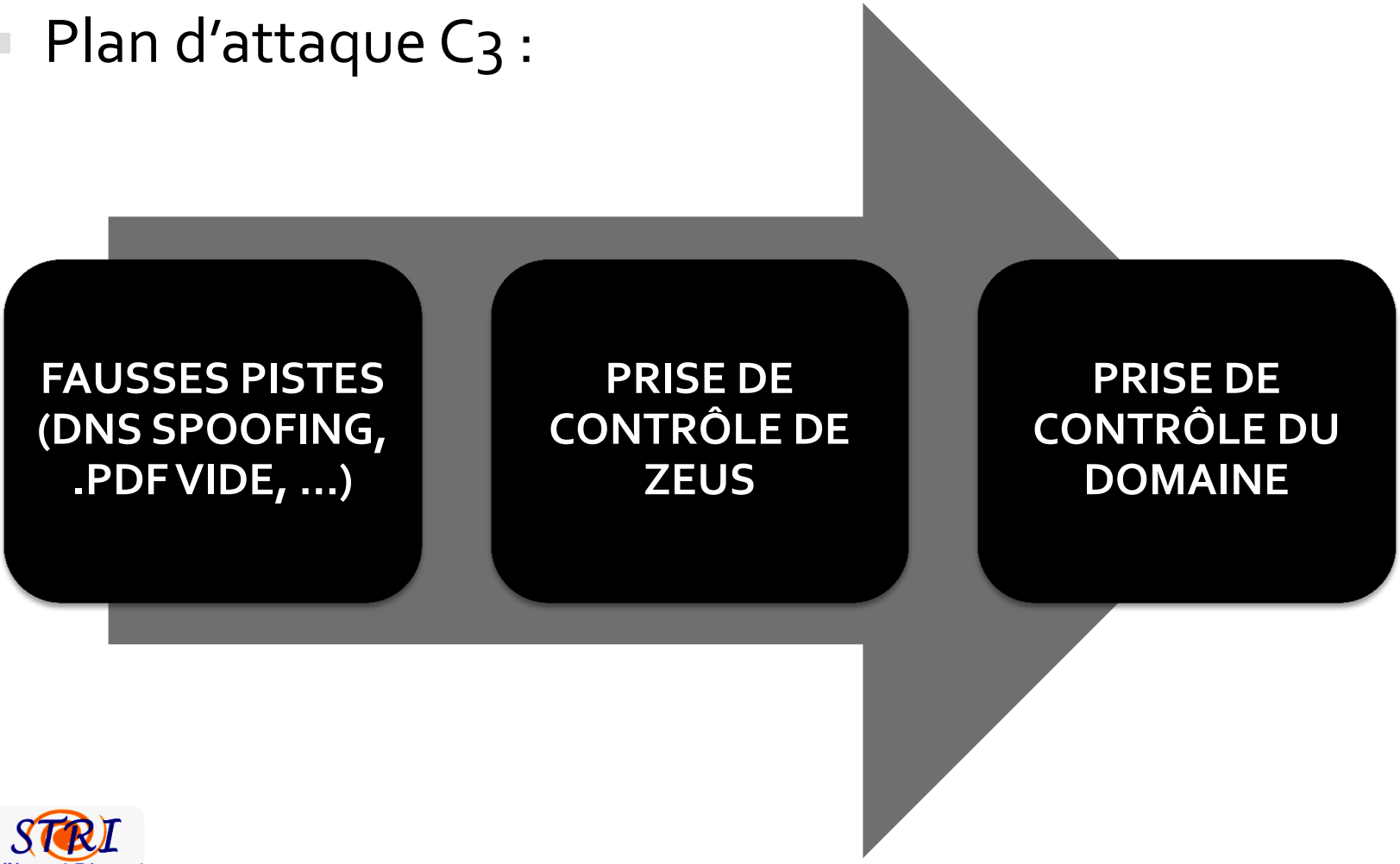
# Deuxième confrontation (C2)

- Bilan de la C2 :
  - **Mêmes problèmes que pour la C1** : perte de temps, etc…
  - Groupe uni et réactif malgré le stress et la tension
  - DNS SPOOFING, c'est toujours du régal !!!
  - **Montée en difficulté** au niveau des attaques (METASPLOIT, etc…)
  - Confiance et expérience emmagasinées pour la dernière confrontation

**À bientôt pour le « SHOW » final qui s'annonce épique…**

# Ultime confrontation (C3)

- Plan d'attaque C3 :

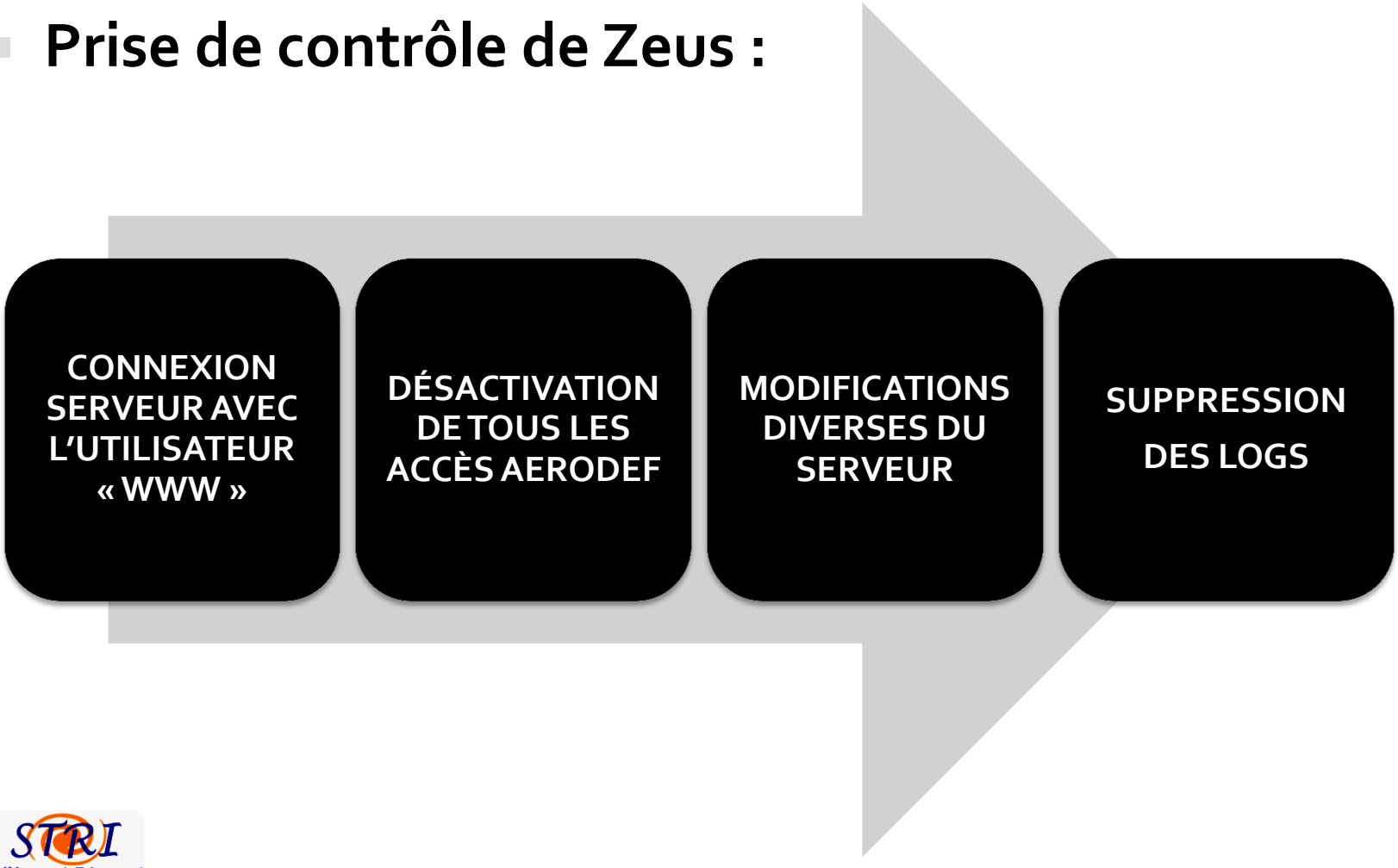


# Ultime confrontation (C3)

- La communication :
  - Responsable de la communication ayant un rôle extrêmement important : **tromper l'adversaire**
    - Faire croire à l'adversaire qu'il s'agit d'une confrontation classique pour **masquer la réalité**
    - Distribution d'un fichier .PDF « vide » pour tromper l'équipe de défense (stress, paranoïa, etc…)
- Au niveau INTERNE : **discrétion !!!**

# Ultime confrontation (C3)

- **Prise de contrôle de Zeus :**



# Ultime confrontation (C3)

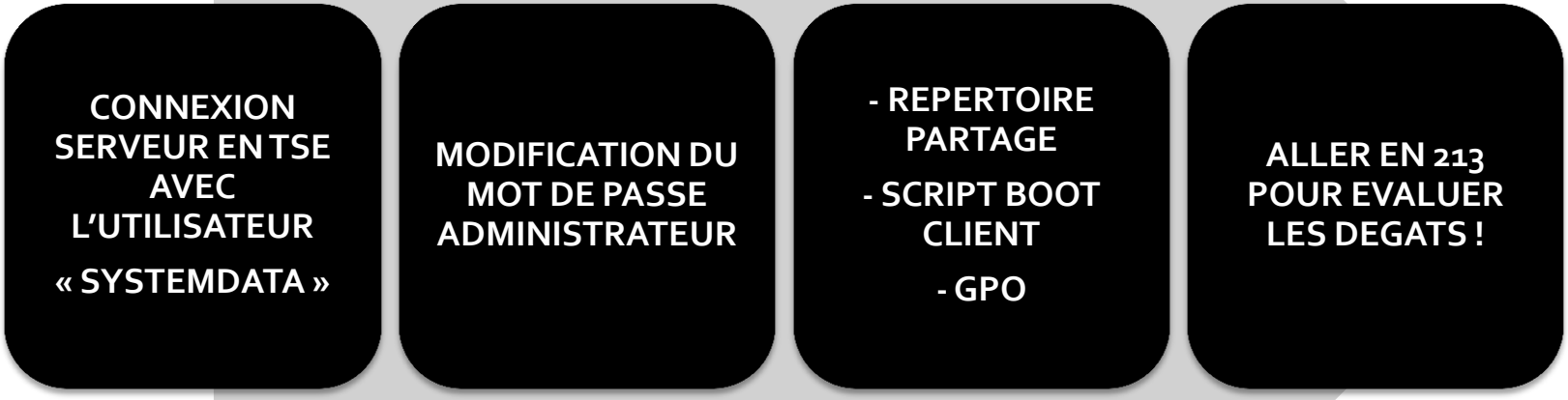
- **Prise de contrôle de Zeus :**
  - Malgré le succès total de l'opération :
    - Extinction manuelle du serveur qui a empêché la suppression des logs + Passage en « Recovery Mod » (Régénération /etc/shadow)

```
root@zeus:/var/www#
Broadcast message from root@zeus (Mon Nov 15 09:43:19 2010):

Power button pressed
The system is going down for system halt NOW!
Connection to 172.30.0.5 closed by remote host.
Connection to 172.30.0.5 closed.
```

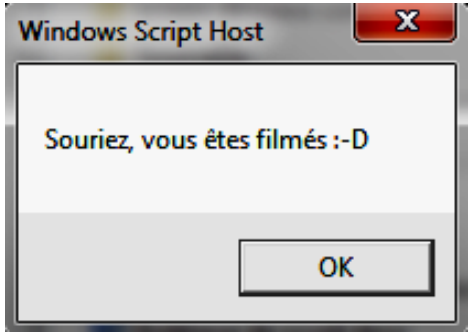
# Ultime confrontation (C3)

- **Prise de contrôle du serveur 2k3 :**



# Ultime confrontation (C3)

- **Prise de contrôle du serveur 2k3 :**
  - 9h45 : Prise de contrôle **mais** aucun client intégré
  - Support de l'équipe Attaque nécessaire pour Aerodef
  - Compréhension de l'ampleur de la confrontation par Aerodef
  - Bingo ! Sauf pour toutes les GPO…



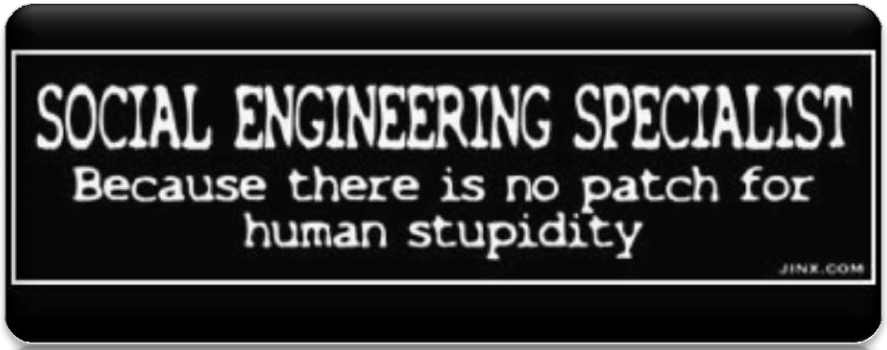

  - Aucun backup du serveur
  - Succès quasi-total
  - Conséquences dramatiques dans le cadre professionnel

# Ultime confrontation (C3)

- Bilan de la C3 :
  - Succès retentissant, **travail de toute une équipe récompensé**
  - Prise de contrôle **TOTALE** du serveur Zeus et du contrôleur de domaine
  - Communication EXTERNE satisfaisante et attaques « trompeuses » réussies
  - On peut donc dire que c'est un… **BOUILLON !!!**

# Quand il n'y en a plus…

- Il faut passer le TOEIC :
  - Tâche de fond basée sur le social engineering :




  - L'IDEE PRINCIPALE ? Créer une « fausse » page Web d'inscription pour une session universitaire du TOEIC

Dans les têtes de tous les étudiants STRI :

**Doit-on le passer obligatoirement ou pas ?**

# Quand il n'y en a plus…

- Il faut passer le TOEIC…
  - Plusieurs étapes :
    - Créer un faux site Web TOEIC où il faudra remplir un formulaire
    - Envoyer le mail avec comme adresse d'expéditeur l'adresse de **M. AOUN, Mme. DEPERETTI** ou encore **Mme. LEROUX**.
    - Héberger ce site sur Internet (toeic-inscriptions.fr par exemple) en espérant que les étudiants ne se rendent pas compte de ce « faux site ».

**IMPORTANT :**
**ne négliger aucun détail !!!**


ETS
TOEIC
Know English. Know Success.
Choisissez votre pays
Accès direct
Recherche
Go
Inscriptions
Vous souhaitez vous inscrire à une session TOEIC® ou TFI™ dans un cadre universitaire. Veuillez remplir le formulaire ci-joint pour créer votre session. Un e-mail de confirmation contenant vos identifiants de session vous sera envoyé dans les plus courts délais.
Civilité :
Monsieur
Prénom :
Nom de famille :
Université :
Email :
Mot de passe :
Pays :
floue
Veuillez entrer ici le mot ou le nombre tel qu'il apparaît dans l'image. Ceci vise à prévenir les abus.
Je souhaiterais recevoir davantage d'informations sur les évaluations et services d' ETS Global (informations marketing comprises)
Envoyer

# Quand il n'y en a plus…

- **Attaque de niveau 1ère section de maternelle !!!**
  - 1) du chapitre 1 « **Sécurisation de base** » du « **Petit Guide pour la sécurité** » d'Alexandre VIARDIN :
    - **Cadenas** sur toutes les machines
    - Désactiver le **boot** sur disquette, CDROM…
    - Mettre un **mot de passe** BIOS
  - Utilisation du live CD « OPHCRACK »
    - Droits administrateur sur les fichiers
    - Récupération des mots de passe (base SAM + Rainbow Tables)
    - Mot de passe BIOS -> Disque dur déporté
  - Pas d'utilisation de ces informations
  - Pas de réitération de ces actions

# Quand il n'y en a plus…

- Bilan : SOCIAL ENGINEERING
  - Communication : THE facteur !!!
  - **Penser avant l'attaque**
  - Manipulation…


**Il est très souvent plus facile d'obtenir des informations intéressantes en usant de son charme et de son phrasé… qu'en s'attaquant au tout dernier routeur CISCO une nuit entière avec son double café en main.**

# Bilan

- Projet passionnant transversal touchant toutes les technologies informatiques des réseaux au système en passant par l'approche humaine
- Gestion de projet de 14 personnes sur 2 mois et demi délicate
- Tentative de motivation en donnant des tâches adaptées en fonction des spécialités
- Bonne coordination nécessaire et surtout de la bonne humeur !
- Système de confrontations délicat : toujours en garder sous la main…
- Tâches de fond réellement passionnantes : se méfier de tout le monde !
- Un réel plaisir malgré une quantité de travail importante !

# MERCI À TOUTES ET À TOUS DE VOTRE ATTENTION