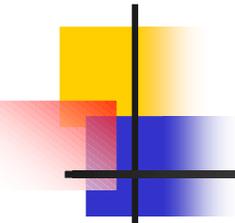


Systemes d'informations: définir le seuil de compétence des acteurs

(s'il existe et si cela est possible, bien entendu...)

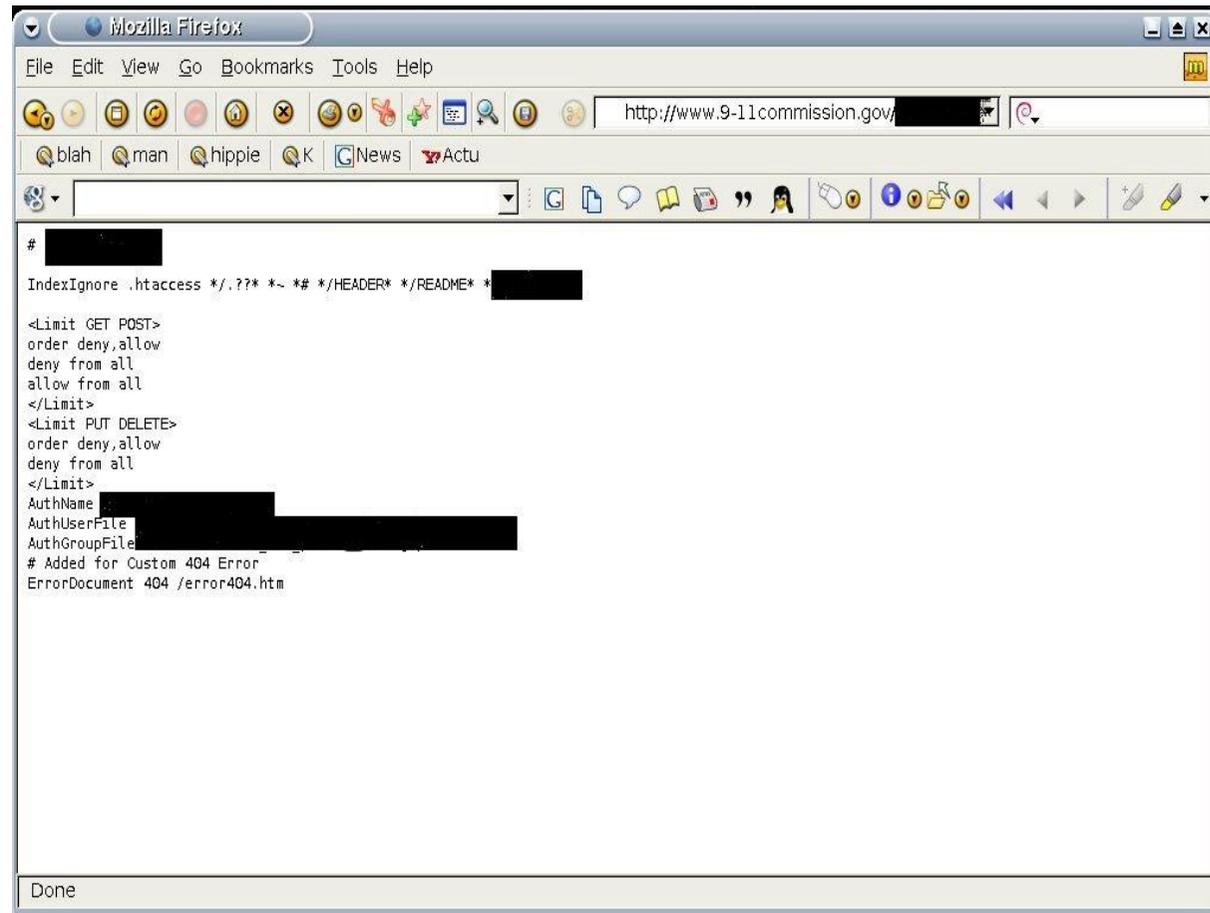


sécurité nulle part?

- n La question d'un développement interne ou externe pour assurer une meilleure sécurité n'est pas neuve...
- n Et s'il n'y avait de sécurité nulle part?
- n Ou presque...

La commission 9/11

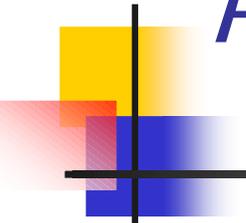
n Développement
maison...



```
# [REDACTED]
IndexIgnore .htaccess */.??* *~ *# */HEADER* */README* * [REDACTED]

<Limit GET POST>
order deny,allow
deny from all
allow from all
</Limit>
<Limit PUT DELETE>
order deny,allow
deny from all
</Limit>
AuthName [REDACTED]
AuthUserFile [REDACTED]
AuthGroupFile [REDACTED]
# Added for Custom 404 Error
ErrorDocument 404 /error404.htm
```

www.kitetoa.com - we will hack
your pizzas for free

The logo graphic consists of a vertical black line intersecting a horizontal black line. To the left of the intersection, there are three overlapping squares: a yellow one at the top, a red one in the middle, and a blue one at the bottom. The text 'Axi.fr' is positioned to the right of the vertical line.

Axi.fr

- n Quelques spams pour des machines à café plus loin...
- n Les fichiers de configuration du système permettant de poster et des milliers d'adresses e-mail.

Axi.fr (suite)

- n Nom de la base
- n Login
- n Password
- n Etc.

```
clean_delay_queueauth 3

## Subscription expiration spool (Cf EXPIRE command)
queueexpire /var/spool/sympa/queueexpire

## Bounce queue
#queuebounce /var/spool/sympa/queuebounce
queuebounce /var/www/bounce/spool

## Outgoing queue
queueoutgoing /var/spool/sympa/queueoutgoing

## Directory for task files created by the task manager
queuetask /var/spool/sympa/queuetask

## Delay between two scan of the main spool (queue). Avoid Zero value !
sleep 5

## Temporary directory
tmpdir /var/spool/sympa/tmp

## S/MIME configuration begin
# DO NOT REMOVE SURROUNDING COMMENTS

# DO NOT MODIFY TEMPLATE VARIABLES
# If you want to reconfigure Sympa for using S/MIME, please run
# dpkg-reconfigure -plow sympam

# Location of the openssl binary
openssl /usr/bin/openssl

# Openssl CA Options
capath /etc/ssl/certs
cafile /usr/share/sympa/ca-bundle.crt

# Password to the lists private key (template variable)
key_passwd [REDACTED]

# SSL certificates directory
ssl_cert_dir /var/lib/sympa/x509-user-certs

## S/MIME configuration end

## Database configuration begin
# DO NOT REMOVE SURROUNDING COMMENTS

# DO NOT EDIT BY HAND
# USE dpkg-reconfigure -plow sympam TO RECONFIGURE

## Database driver (DBD)
db_type [REDACTED]

## Name of your database
db_name [REDACTED]

## Your database hostname
db_host [REDACTED]

## Username to connect to the DB
db_user [REDACTED]

## Password for the user
db_passwd [REDACTED]

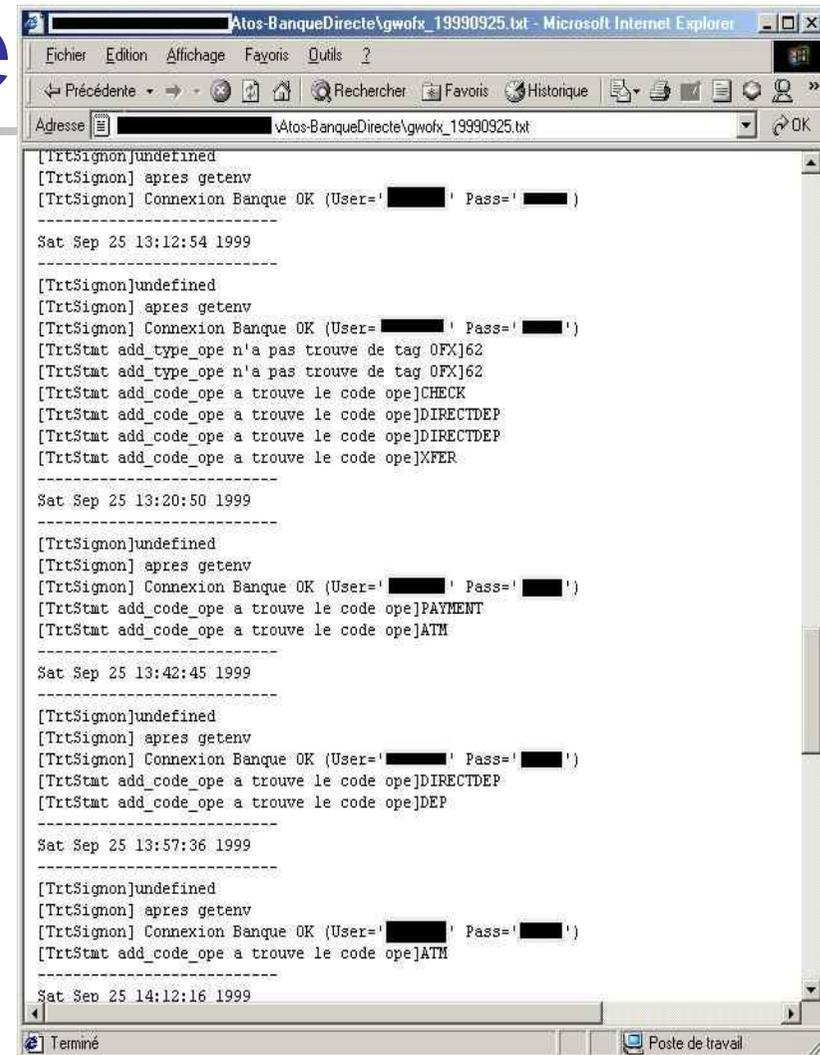
## Database options
db_options [REDACTED]

## Database configuration end

Terminé 217.174.197.8
```

Banque Directe

n Développement externe...



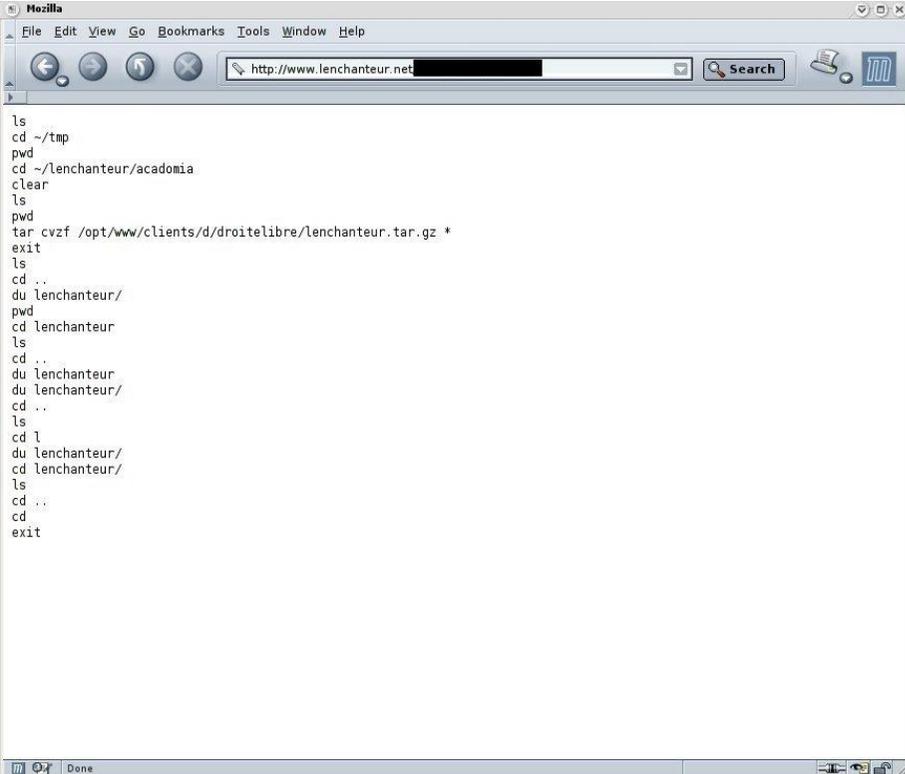
```
Atos-BanqueDirecte\gwofx_19990925.txt - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Recherche Favoris Historique
Adresse \Atos-BanqueDirecte\gwofx_19990925.txt OK

[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User='[REDACTED]' Pass='[REDACTED]')
-----
Sat Sep 25 13:12:54 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User='[REDACTED]' Pass='[REDACTED]')
[TrtStat add_type_ope n'a pas trouve de tag OFX]62
[TrtStat add_type_ope n'a pas trouve de tag OFX]62
[TrtStat add_code_ope a trouve le code ope]CHECK
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]XFER
-----
Sat Sep 25 13:20:50 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User='[REDACTED]' Pass='[REDACTED]')
[TrtStat add_code_ope a trouve le code ope]PAYMENT
[TrtStat add_code_ope a trouve le code ope]ATM
-----
Sat Sep 25 13:42:45 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User='[REDACTED]' Pass='[REDACTED]')
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]DEP
-----
Sat Sep 25 13:57:36 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User='[REDACTED]' Pass='[REDACTED]')
[TrtStat add_code_ope a trouve le code ope]ATM
-----
Sat Sep 25 14:12:16 1999
-----
Terminé Poste de travail
```

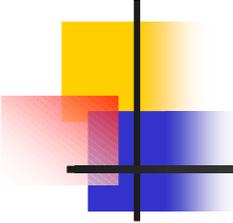
www.kitetoa.com - we will hack
your pizzas for free

Sarkospam: maison ou externe?

- n L'enchanteur Nouveaux Médias: externe ou interne ?
- n Ce fichier laisse entendre que des données ont été fournies par la Droite Libre



```
ls
cd ~/tmp
pwd
cd ~/lenchanteur/acadomia
clear
ls
pwd
tar cvzf /opt/www/clients/d/droitelibre/lenchanteur.tar.gz *
exit
ls
cd ..
du lenchanteur/
pwd
cd lenchanteur
ls
cd ..
du lenchanteur
du lenchanteur/
cd ..
ls
cd l
du lenchanteur/
cd lenchanteur/
ls
cd ..
cd
exit
```

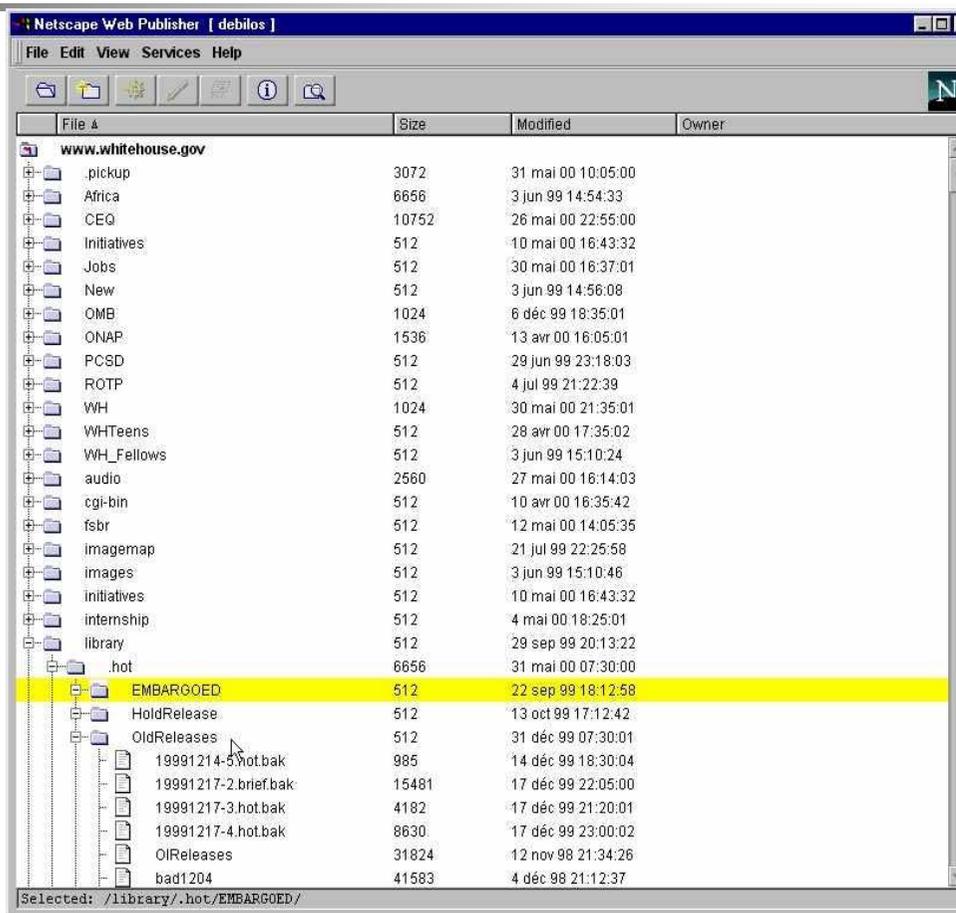


Le grand méchant Net

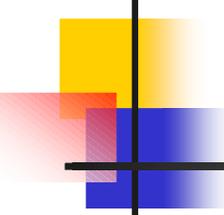
- n Combien de millions dépensés pour protéger la porte qui relie l'entreprise à Internet...?
- n Il existe d'autres portes
- n Pourquoi cette focalisation?

Porte blindée, murs en carton

n Blinder la porte ne suffisait pas, même à la Maison-Blanche...



www.kitetoa.com - we will hack
your pizzas for free



Porte blindée, murs en carton II

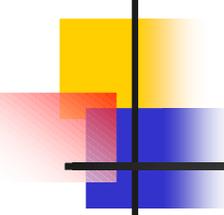
n Blinder la porte ne suffit toujours pas...

Lance Armstrong

n Quelques milliers
d'e-mails a
disposition des
spammers.

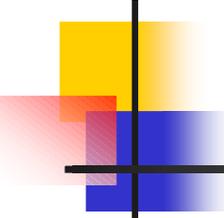
```
- <viewentries t
- <viewentry p children="4" descendants="4" siblings="6152">
- <entrydata " category="true">
<text>199
</entrydata
- <entrydata
<number
</entrydata
</viewentry>
- <viewentry p A44F96BA86256BF9001D44ED" noteid="2136" siblings="4">
- <entrydata 444F96BA86256BF9001D44ED" name">
<text>Ca
</entrydata
- <entrydata
<text/>
</entrydata
</viewentry>
- <viewentry p 6ACF435286256BFA0063D15A" noteid="7DC2" siblings="4">
- <entrydata 6ACF435286256BFA0063D15A" name">
<text>Ca
</entrydata
- <entrydata
<text/>
</entrydata
</viewentry>
- <viewentry p 3E52B3E86256BFB00602A1E" noteid="BE96" siblings="4">
- <entrydata 3E52B3E86256BFB00602A1E" name">
<text>Ca
</entrydata
- <entrydata
<text/>
</entrydata
</viewentry>
- <viewentry p 719E1C3386256BFC001FD3CE" noteid="DB3A" siblings="4">
- <entrydata 719E1C3386256BFC001FD3CE" name">
<text>Ca
</entrydata
- <entrydata
<text/>
</entrydata
</viewentry>
- <viewentry p children="3" descendants="3" siblings="6152">
- <entrydata " category="true">
<text>1f
</entrydata
- <entrydata
<number
</entrydata
```

www.kitetoa.com - we will hack
your pizzas for free



Classique ou Hippie?

- n En matière de tests d'intrusion, vous êtes plutôt classique ou hippie?
- n Le concept de hacking de pizzas
- n Comment est-il possible que Kitettoa.com existe...
- n Alors que nous n'avons pas de capacités techniques particulières...



So what?

- n Que faire?
- n Existe-t-il un moyen de sécuriser un réseau, une application web, etc.?
- n La responsabilité des directions générales.
- n La conclusion à laquelle les hackers de pizzas sont arrivés...