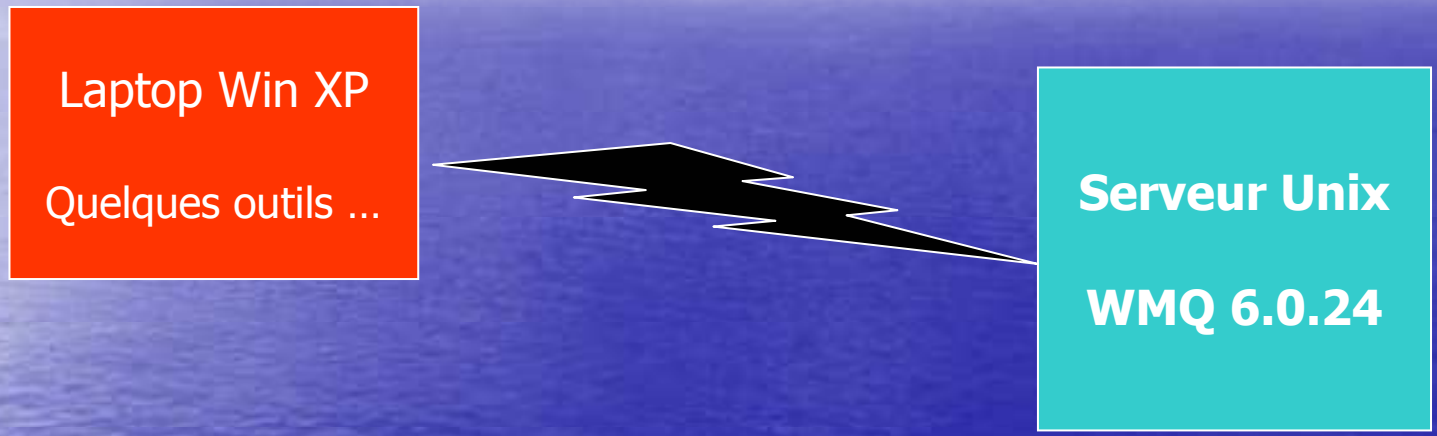
WebSphere. software

Votre réseau MQ est-il « *secure* » ?

ou « L'histoire des trois petits Qmgrs »

Luc-Michel Demey
Demey® Consulting
lmd@demey-consulting.fr

Configuration utilisée

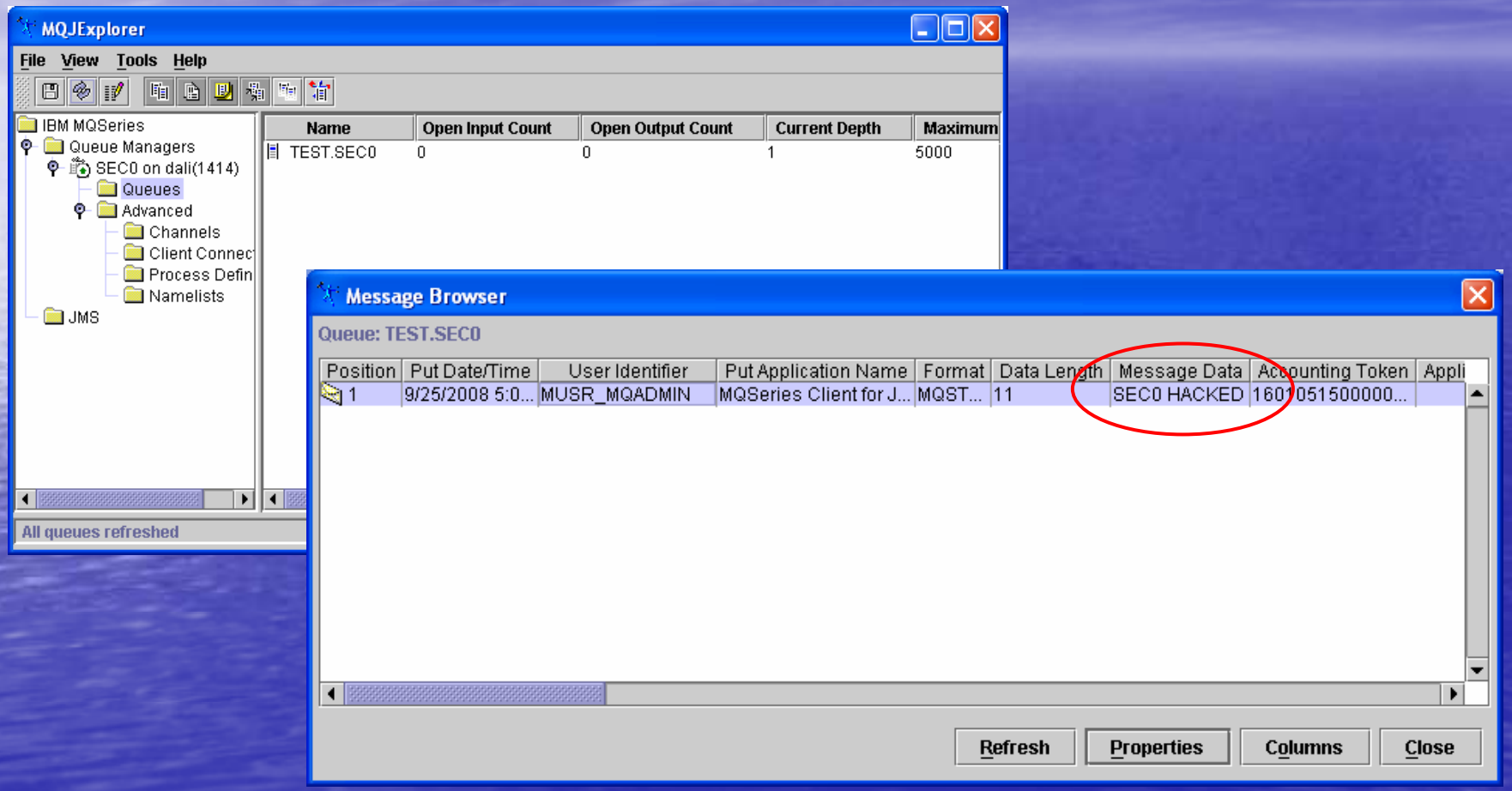


Hypothèse de base : l'attaquant à un accès IP à l'attaqué.

Test n°1

- Adresse IP connue, port connu, nom QM connu :
  - SEC0
  - Sur 192.168.0.8
  - Port du listener : 1414
- Utilisation MQJE depuis un poste Windows
  - Utilise le canal SYSTEM.ADMIN.SVRCONN
- Résultat : Full Access
  - Sans authentification sur le serveur Unix
  - Le « hacker » a les droits « mqm » sur le serveur
    (en fait les droit du compte sous lequel s'exécute le listener)

Prise de contrôle de SEC0



Ensuite ?

- Il y a d'autres Qmgr sur le réseau, mais …
  - adresse IP non connue
  - port listener non connu
  - nom Qmgr non connu
  - canaux SVRCONN non connus
  - …

→Utilisation d'un outil de scan MQ Open Source

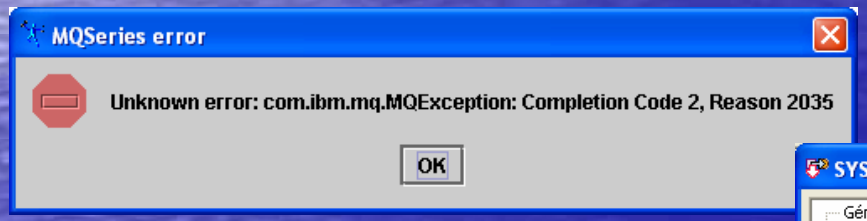
(merci Roger Lacroix !)

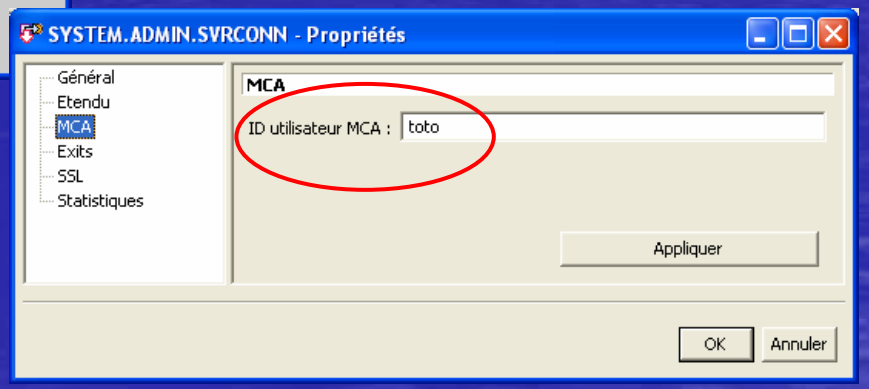
Résultat

QMgrName,Version,ChannelName,hostname/IP_Address,Port
SEC0,600,SYSTEM.DEF.SVRCONN,192.168.0.8,1414
SEC0,600,SYSTEM.AUTO.SVRCONN,192.168.0.8,1414
SEC0,600,SYSTEM.ADMIN.SVRCONN,192.168.0.8,1414
SEC1,600,SYSTEM.DEF.SVRCONN,192.168.0.8,1501
SEC1,600,SYSTEM.AUTO.SVRCONN,192.168.0.8,1501
SEC1,600,SYSTEM.ADMIN.SVRCONN,192.168.0.8,1501
SEC2,600,SYSTEM.DEF.SVRCONN,192.168.0.8,1502
SEC2,600,SYSTEM.AUTO.SVRCONN,192.168.0.8,1502
SEC2,600,SYSTEM.ADMIN.SVRCONN,192.168.0.8,1502
SEC2,600,ADMIN.SVRCONN,192.168.0.8,1502
SEC3,600,SYSTEM.DEF.SVRCONN,192.168.0.8,1503
SEC3,600,SYSTEM.AUTO.SVRCONN,192.168.0.8,1503
SEC3,600,ADMIN.SSL,192.168.0.8,1503
...

Test n°2 : Attaque SEC1

- Adresse IP connue, port connu, nom QM connu :
  - SEC1
  - Sur 192.168.0.8
  - Port du listener : 1501
- Utilisation MQJE depuis un poste Windows
- Résultat : 2035 - Denied, car le canal SYSTEM.ADMIN.SVRCONN contient un MCAUSER invalide



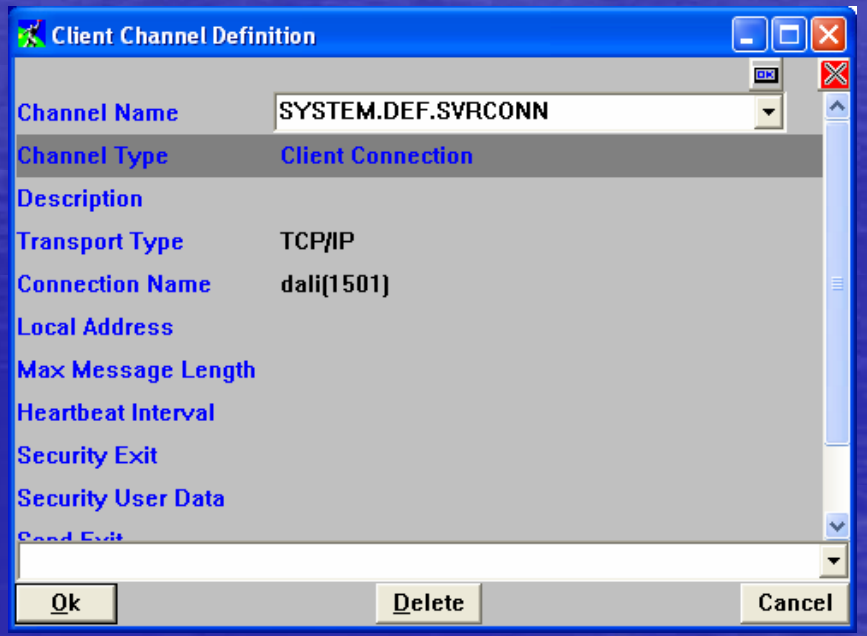


Variante : Suppression du canal

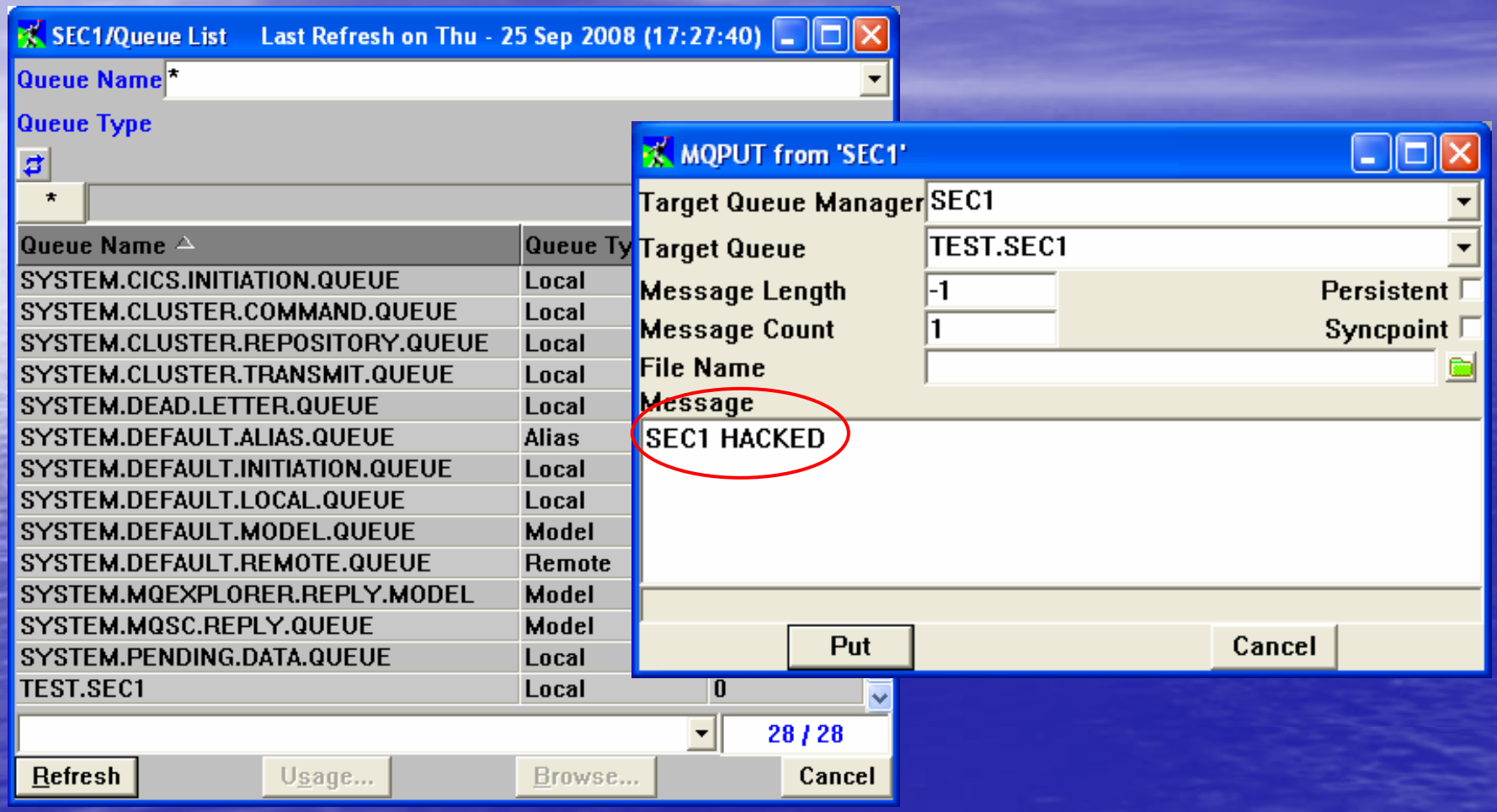
Attaque SEC1 : alternative

Utilisation des objets par défaut

- Création d'un compte « mqm » sur le laptop
- Utilisation du MO71
- Entrée par le canal SYSTEM.DEF.SVRCONN
  - paramètre MCAUSER = ' '



Prise de contrôle de SEC1



Attaque SEC2

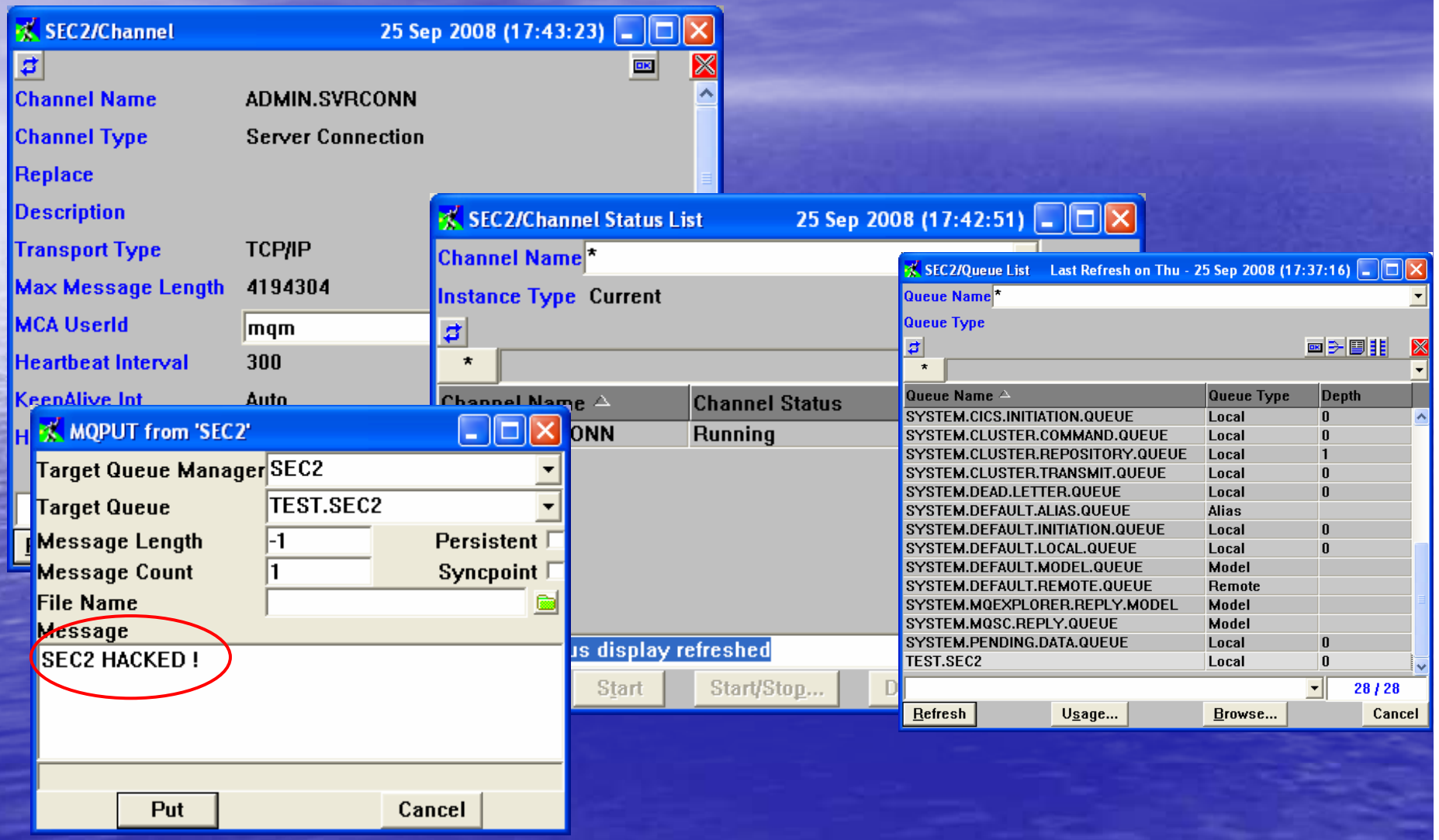
Ou les « avantages » de la sécurité par l'obscurité …

- Configuration :

  SEC2,600,ADMIN.SVRCONN,192.168.0.8,1502

- Canal SVRCONN spécifique pour l'administration
  - Avec MCAUSER = « mqm »

Prise de contrôle de SEC2



Attaque SEC3

… ou l'histoire du Qmgr qui se croyait en sécurité …

- Configuration :
  - Canaux SVRCONN par défaut « fermés »
  - Canal d'administration spécifique protégé par SSL
    - Attention si WMQ < 6.0.2.2 → bug « DEFCON »
- Qmgr inviolable ?

Attaque SEC3

Attaque « par le jardin »

- Création d'un Qmgr sur le laptop
- Transformation du [illegible] en [illegible]
- Modification du [illegible] sur SEC3
- Création d'une [illegible]
- Démarrage d[illegible]nal [illegible]

→ Possibi[illegible]ue déposer des messages [illegible] à condition d'en connaître le nom …

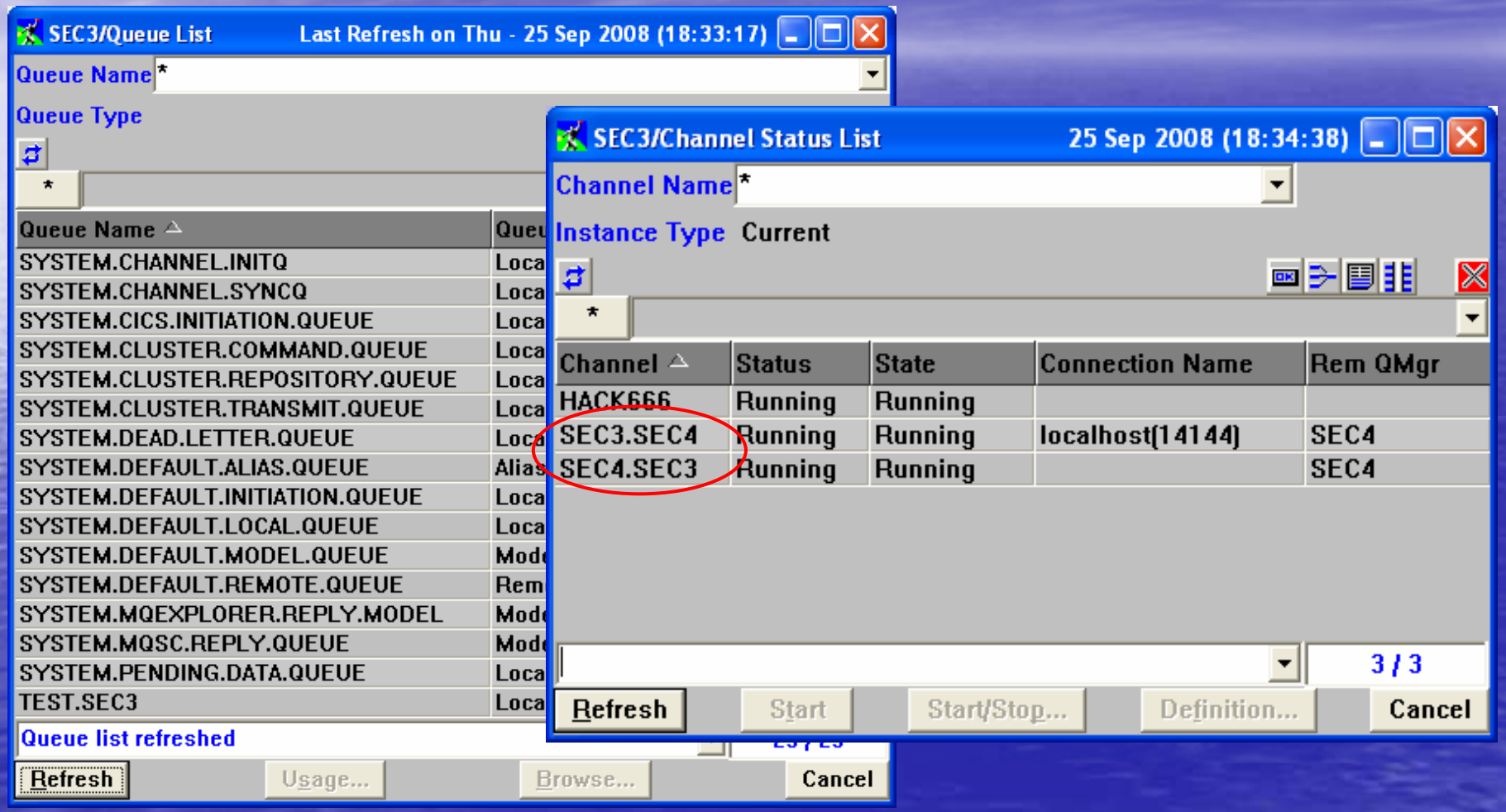
Cette partie de la présentation a été volontairement brouillée

Attaque SEC3

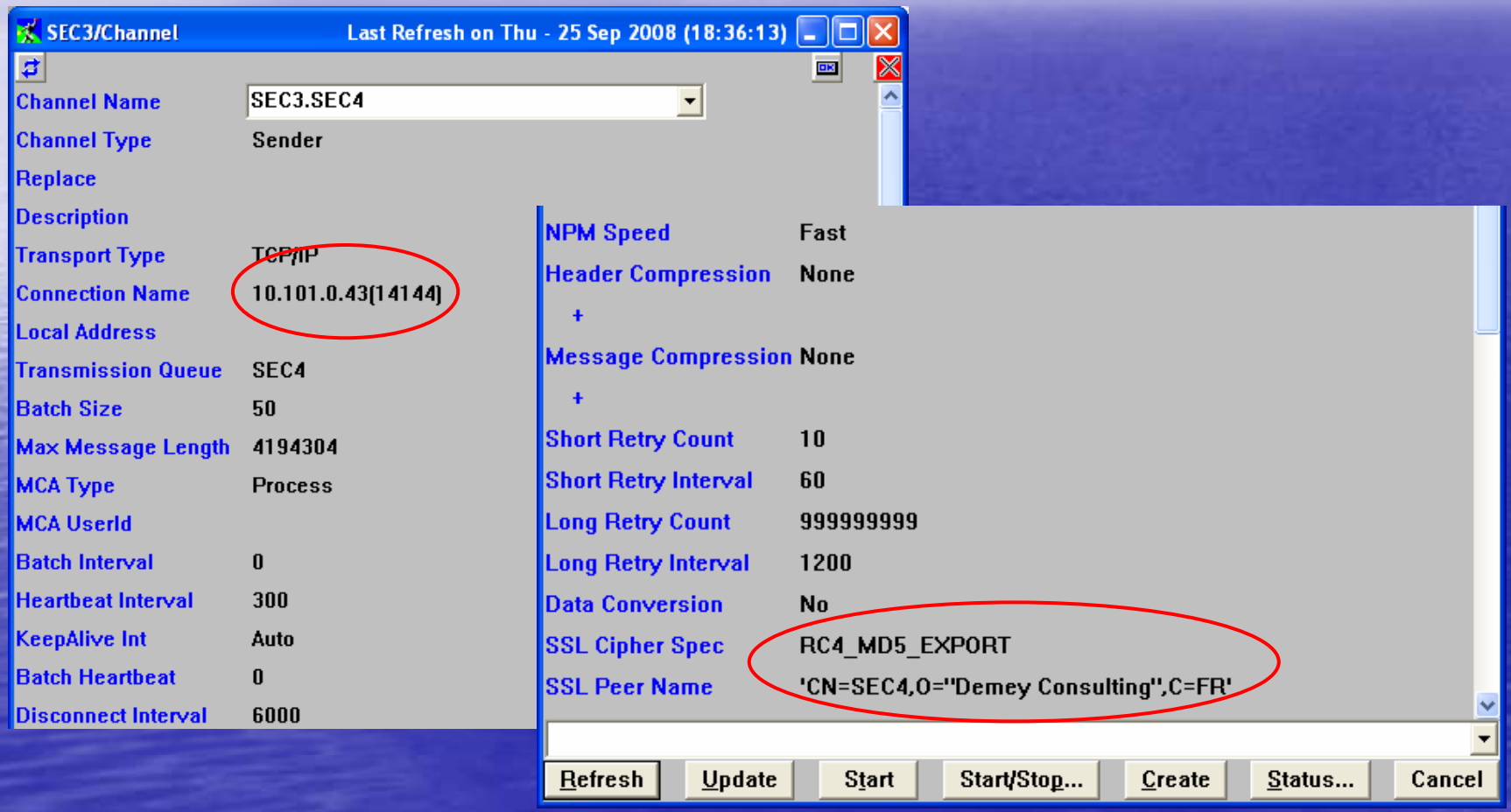
- Création d'une file éloignée pointant sur l[illegible] de SEC3
- Dépôt d'un message PCF forgé [illegible]
- Ce message demande la cré[illegible]on d'un canal SVRCONN « [illegible] », avec [illegible] paramètre MCAUSER à « [illegible] »
- Utilisation du M[illegible]1 pour se connecter à SEC3

Cette partie de la présentation a été volontairement brouillée

Prise de contrôle SEC3



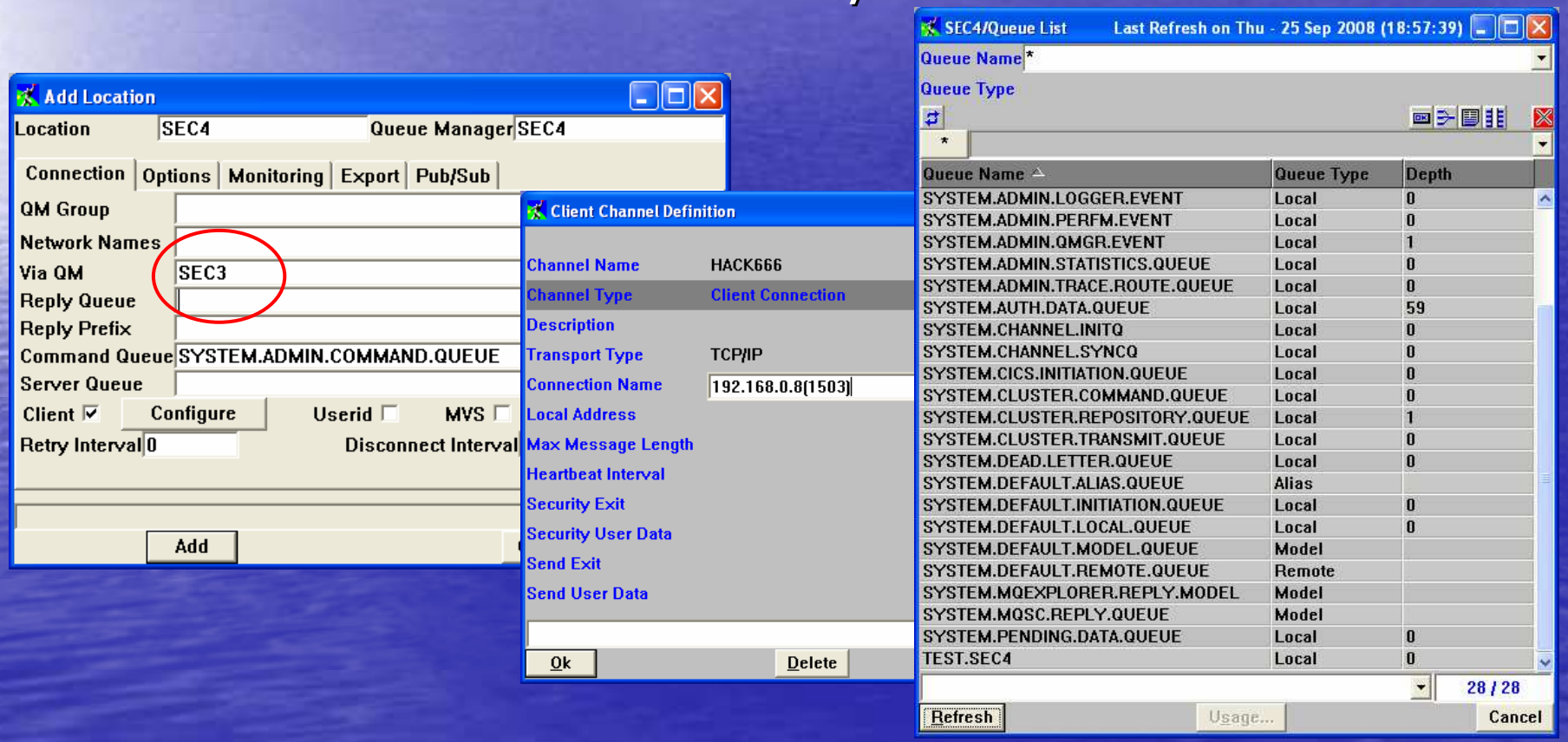
Liaison SEC3 → SEC4



Attaque SEC4

Attaque « par rebond »

- Utilisation de la fonction Proxy du MO71



Bilan des risques

- Absence de sécurité
  - Installation de base
- Aggravation du risque
  - Ajout d'un MCAUSER
- Sécurité par l'obscurité
  - Création d'un canal spécifique
- Objets par défaut
  - Ne rien oublier
- Accès de type proxy
  - Un risque pour les liens inter-sociétés

Solutions ?

- Serveurs MQ en DMZ applicative
- Neutraliser les objets par défaut
- Identifier les partenaires via SSL
- MCAUSER systématique
- Droits d'accès aux objets
- Audits réguliers