

Votre réseau MQ est-il « *secure* » ?

OU « *L'histoire des trois petits Qmgrs* »

# Configuration utilisée

Laptop Win XP  
Quelques outils ...



Serveur Unix  
WMQ 6.0.24

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

# Test n°1

- Adresse IP connue, port connu, nom QM connu :
  - SECO
  - 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 SECO

The screenshot displays two windows from the IBM MQ Explorer interface. The 'MQ Explorer' window shows a tree view of the queue manager 'SECO on dali(1414)' and a table of queue statistics. The 'Message Browser' window shows a message in the 'TEST.SECO' queue, with the message data 'SECO HACKED' circled in red.

**MQ Explorer Queue Statistics Table:**

Name	Open Input Count	Open Output Count	Current Depth	Maximum
TEST.SECO	0	0	1	5000

**Message Browser Message Table:**

Position	Put Date/Time	User Identifier	Put Application Name	Format	Data Length	Message Data	Accounting Token	Appli
1	9/25/2008 5:0...	MUSR_MQADMIN	MQSeries Client for J...	MQST...	11	SECO HACKED	1601051500000...	

## 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 !)

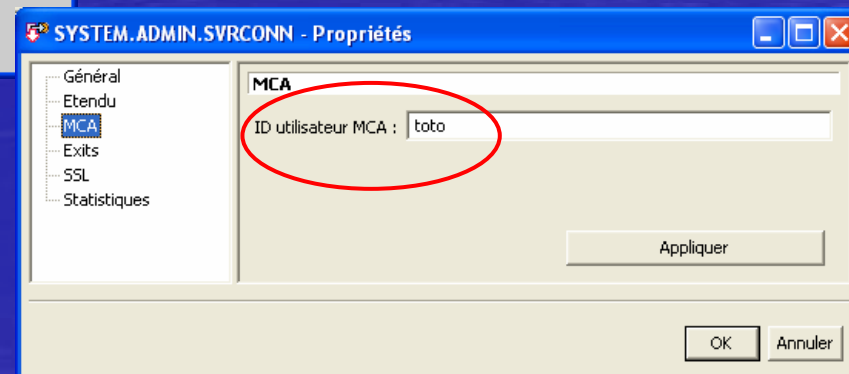
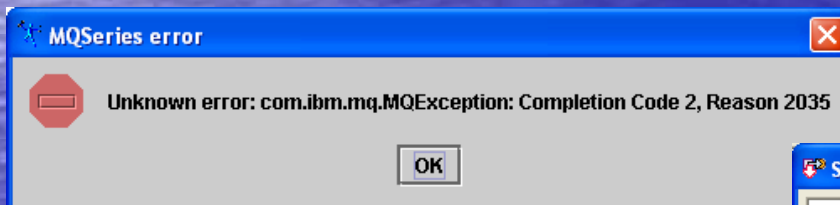
# Résultat

```
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





# Prise de contrôle de SEC1

The screenshot shows two windows from the IBM MQ console. The background window is titled "SEC1/Queue List" and displays a table of system queues. The foreground window is titled "MQPUT from 'SEC1'" and shows the configuration for putting a message into the "TEST.SEC1" queue. The message content is "SEC1 HACKED", which is circled in red.

Queue Name	Queue Type
SYSTEM.CICS.INITIATION.QUEUE	Local
SYSTEM.CLUSTER.COMMAND.QUEUE	Local
SYSTEM.CLUSTER.REPOSITORY.QUEUE	Local
SYSTEM.CLUSTER.TRANSMIT.QUEUE	Local
SYSTEM.DEAD.LETTER.QUEUE	Local
SYSTEM.DEFAULT.ALIAS.QUEUE	Alias
SYSTEM.DEFAULT.INITIATION.QUEUE	Local
SYSTEM.DEFAULT.LOCAL.QUEUE	Local
SYSTEM.DEFAULT.MODEL.QUEUE	Model
SYSTEM.DEFAULT.REMOTE.QUEUE	Remote
SYSTEM.MQEXPLORER.REPLY.MODEL	Model
SYSTEM.MQSC.REPLY.QUEUE	Model
SYSTEM.PENDING.DATA.QUEUE	Local
TEST.SEC1	Local

MQPUT from 'SEC1'

Target Queue Manager: SEC1

Target Queue: TEST.SEC1

Message Length: -1  Persistent

Message Count: 1  Syncpoint

File Name:

Message: **SEC1 HACKED**

Buttons: Put, Cancel

# 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

The screenshot displays four overlapping windows from the IBM MQ console:

- SEC2/Channel**: Shows configuration for channel ADMIN.SVRCONN, a Server Connection using TCP/IP transport, with a Max Message Length of 4194304 and MCA Userid 'mqm'.
- SEC2/Channel Status List**: Shows a table with columns 'Channel Name' and 'Channel Status'. The entry 'ADMIN.SVRCONN' is listed with a status of 'Running'.
- SEC2/Queue List**: Shows a table with columns 'Queue Name', 'Queue Type', and 'Depth'. The entry 'TEST.SEC2' is listed with a Local queue type and a depth of 0.
- MQPUT from 'SEC2'**: A dialog box for putting a message. The 'Message' field contains the text 'SEC2 HACKED!', which is circled in red. Other fields include 'Target Queue Manager' (SEC2), 'Target Queue' (TEST.SEC2), 'Message Length' (-1), and 'Message Count' (1).

# 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 `channelName` en `channelName`, `channelName` `channelName`, `channelName` `channelName`, `channelName` `channelName`
  - Modification du `channelName` `channelName` sur SEC3
  - Création d'une `channelName`
  - Démarrage d'un canal `channelName`
- Possibilité de déposer des messages `channelName` `channelName` `channelName`  
 condition d'en connaître le nom ...

**Cette partie de la présentation a été volontairement brouillée**



# Prise de contrôle SEC3

SEC3/Queue List      Last Refresh on Thu - 25 Sep 2008 (18:33:17)

Queue Name \*

Queue Type

Queue Name ^	Queue Type
SYSTEM.CHANNEL.INITQ	Local
SYSTEM.CHANNEL.SYNCQ	Local
SYSTEM.CICS.INITIATION.QUEUE	Local
SYSTEM.CLUSTER.COMMAND.QUEUE	Local
SYSTEM.CLUSTER.REPOSITORY.QUEUE	Local
SYSTEM.CLUSTER.TRANSMIT.QUEUE	Local
SYSTEM.DEAD.LETTER.QUEUE	Local
SYSTEM.DEFAULT.ALIAS.QUEUE	Alias
SYSTEM.DEFAULT.INITIATION.QUEUE	Local
SYSTEM.DEFAULT.LOCAL.QUEUE	Local
SYSTEM.DEFAULT.MODEL.QUEUE	Model
SYSTEM.DEFAULT.REMOTE.QUEUE	Remote
SYSTEM.MQEXPLORER.REPLY.MODEL	Model
SYSTEM.MQSC.REPLY.QUEUE	Model
SYSTEM.PENDING.DATA.QUEUE	Local
TEST.SEC3	Local

Queue list refreshed

Refresh      Usage...      Browse...      Cancel

SEC3/Channel Status List      25 Sep 2008 (18:34:38)

Channel Name \*

Instance Type Current

Channel ^	Status	State	Connection Name	Rem QMgr
HACK666	Running	Running		
SEC3.SEC4	Running	Running	localhost(14144)	SEC4
SEC4.SEC3	Running	Running		SEC4

Refresh      Start      Start/Stop...      Definition...      Cancel

# Liaison SEC3 → SEC4

SEC3/Channel Last Refresh on Thu - 25 Sep 2008 (18:36:13)

Channel Name: SEC3.CHANNEL

Channel Type: Sender

Replace: [ ]

Description: [ ]

Transport Type: TCP/IP

Connection Name: 10.101.0.43[14144]

Local Address: [ ]

Transmission Queue: SEC4

Batch Size: 50

Max Message Length: 4194304

MCA Type: Process

MCA UserId: [ ]

Batch Interval: 0

Heartbeat Interval: 300

KeepAlive Int: Auto

Batch Heartbeat: 0

Disconnect Interval: 6000

NPM Speed: Fast

Header Compression: None

+ [ ]

Message Compression: None

+ [ ]

Short Retry Count: 10

Short Retry Interval: 60

Long Retry Count: 999999999

Long Retry Interval: 1200

Data Conversion: No

SSL Cipher Spec: RC4\_MD5\_EXPORT

SSL Peer Name: 'CN=SEC4,O="Demey Consulting",C=FR'

Refresh Update Start Start/Stop... Create Status... Cancel



# Attaque SEC4

## Attaque « par rebond »

- Utilisation de la fonction Proxy du MO71

**Add Location**

Location: SEC4 Queue Manager: SEC4

Connection Options Monitoring Export Pub/Sub

QM Group

Network Names

Via QM: SEC3

Reply Queue

Reply Prefix

Command Queue: SYSTEM.ADMIN.COMMAND.QUEUE

Server Queue

Client  Configure Userid  MVS

Retry Interval: 0 Disconnect Interval

Add

**Client Channel Definition**

Channel Name: HACK666

Channel Type: Client Connection

Description

Transport Type: TCP/IP

Connection Name: 192.168.0.8[1503]

Local Address

Max Message Length

Heartbeat Interval

Security Exit

Security User Data

Send Exit

Send User Data

Ok Delete

**SEC4/Queue List** Last Refresh on Thu - 25 Sep 2008 (18:57:39)

Queue Name\*

Queue Type

Queue Name	Queue Type	Depth
SYSTEM.ADMIN.LOGGER.EVENT	Local	0
SYSTEM.ADMIN.PERFM.EVENT	Local	0
SYSTEM.ADMIN.QMGR.EVENT	Local	1
SYSTEM.ADMIN.STATISTICS.QUEUE	Local	0
SYSTEM.ADMIN.TRACE.ROUTE.QUEUE	Local	0
SYSTEM.AUTH.DATA.QUEUE	Local	59
SYSTEM.CHANNEL.INITQ	Local	0
SYSTEM.CHANNEL.SYNCQ	Local	0
SYSTEM.CICS.INITIATION.QUEUE	Local	0
SYSTEM.CLUSTER.COMMAND.QUEUE	Local	0
SYSTEM.CLUSTER.REPOSITORY.QUEUE	Local	1
SYSTEM.CLUSTER.TRANSMIT.QUEUE	Local	0
SYSTEM.DEAD.LETTER.QUEUE	Local	0
SYSTEM.DEFAULT.ALIAS.QUEUE	Alias	
SYSTEM.DEFAULT.INITIATION.QUEUE	Local	0
SYSTEM.DEFAULT.LOCAL.QUEUE	Local	0
SYSTEM.DEFAULT.MODEL.QUEUE	Model	
SYSTEM.DEFAULT.REMOTE.QUEUE	Remote	
SYSTEM.MQEXPLORER.REPLY.MODEL	Model	
SYSTEM.MQSC.REPLY.QUEUE	Model	
SYSTEM.PENDING.DATA.QUEUE	Local	0
TEST.SEC4	Local	0

28 / 28

Refresh Usage... Cancel

# 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