The Top Security Risks Auditors Complain About and How to Tackle Them

COMMON Luxembourg
28 Sept. 2017

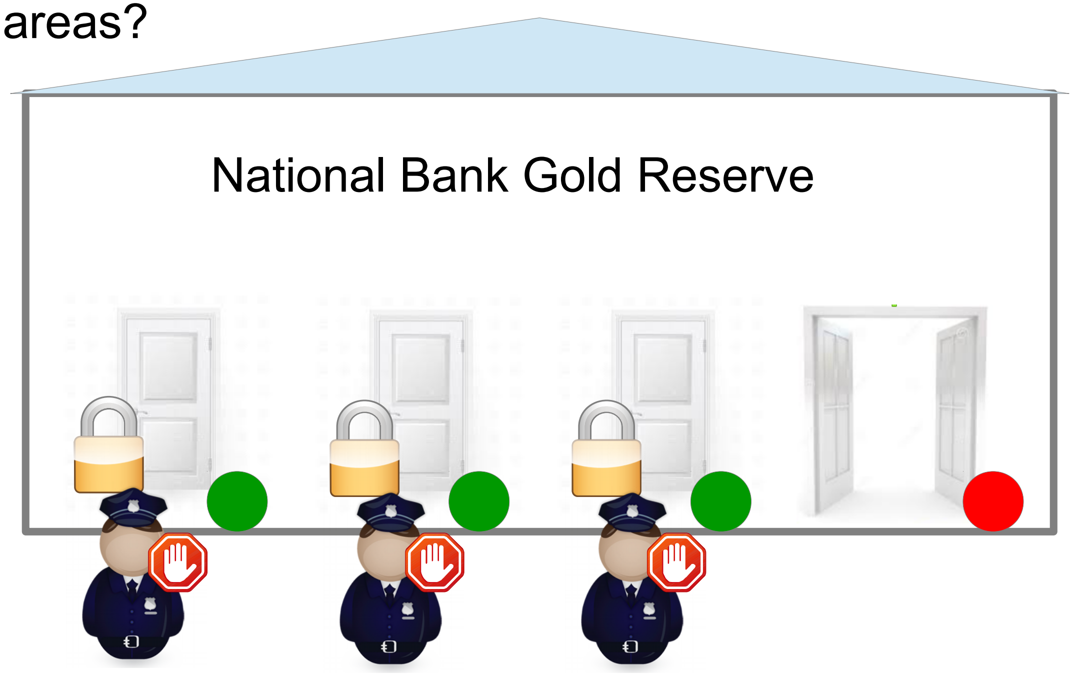
Thomas Barlen
Senior Managing Consultant
barlen@de.ibm.com

Agenda

- Common findings during a security assessment
- Addressing identified high risks
- Compliance monitoring

Security and risk management

- Security is all about managing risks
- Security assessments can provide a snapshot of the security state of a system
  - Identified risks can have different severity levels depending on the probability of exploitation and the associated cost
- Why might be a system at a high risk level when most areas indicate no risk or just a few low risk areas?



Outcome of a security assessment or audit

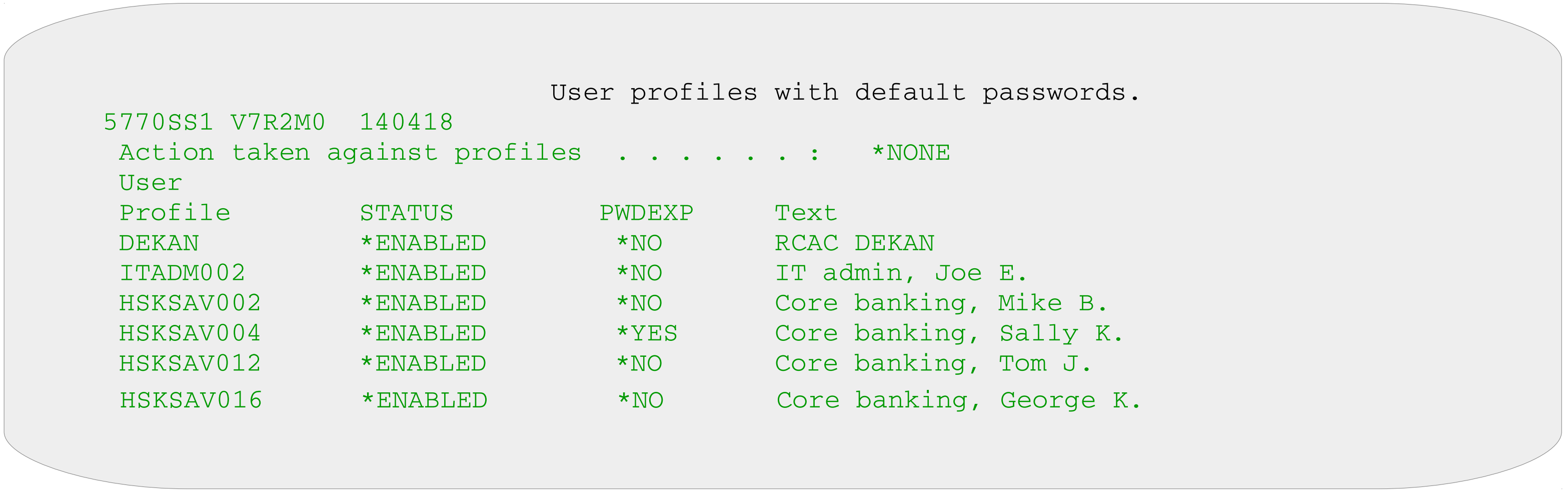
- A security assessment can reveal security weaknesses/risks, i.e. in configurations or application design
- A business audit takes a look from a different angle but also shows IT security issues
- Both consider compliance requirements, i.e.
  - corporate security policies
  - government regulations (i.e. SOX)
  - industry-specific regulations (i.e. PCI DSS)
- Some of the identified risks of an audit or assessment can be easily exploited to gain unauthorized access, perform data theft or manipulation, or cause a service disruption
  - many of the findings can be found in almost every company

Common findings

- Default passwords
- Publicy authorized user profiles
- DDM access without authentication
- SSH access for all user profiles
- High number of users with special authorities
- Public authorities on custom created objects
- Unused network services and default configurations

Default passwords

- Easy exploitation to gain access to a system
- On most examined systems, users with default passwords also have special authorities including *ALLOBJ
  - assessments show from a few to 1000s of profiles with default passwords
- Default passwords mostly caused by IT personnel
  - can provide any password
  - passwords do not have to comply with password policies
- Analyze default password (ANZDFTPWD) can show affected user profiles



```
                              User profiles with default passwords.
5770SS1 V7R2M0  140418
 Action taken against profiles  . . . . . . . :    *NONE
 User
 Profile         STATUS         PWDEXP     Text
 DEKAN           *ENABLED        *NO       RCAC DEKAN
 ITADM002        *ENABLED        *NO       IT admin, Joe E.
 HSKSAV002       *ENABLED        *NO       Core banking, Mike B.
 HSKSAV004       *ENABLED        *YES      Core banking, Sally K.
 HSKSAV012       *ENABLED        *NO       Core banking, Tom J.
 HSKSAV016       *ENABLED        *NO       Core banking, George K.
```

Default passwords - recommendations

- Define password policies via the QPWDRULES system value
  - include the *ALLCRTCHG configuration value to enforce policies also for administrators (V7R2 and higher)

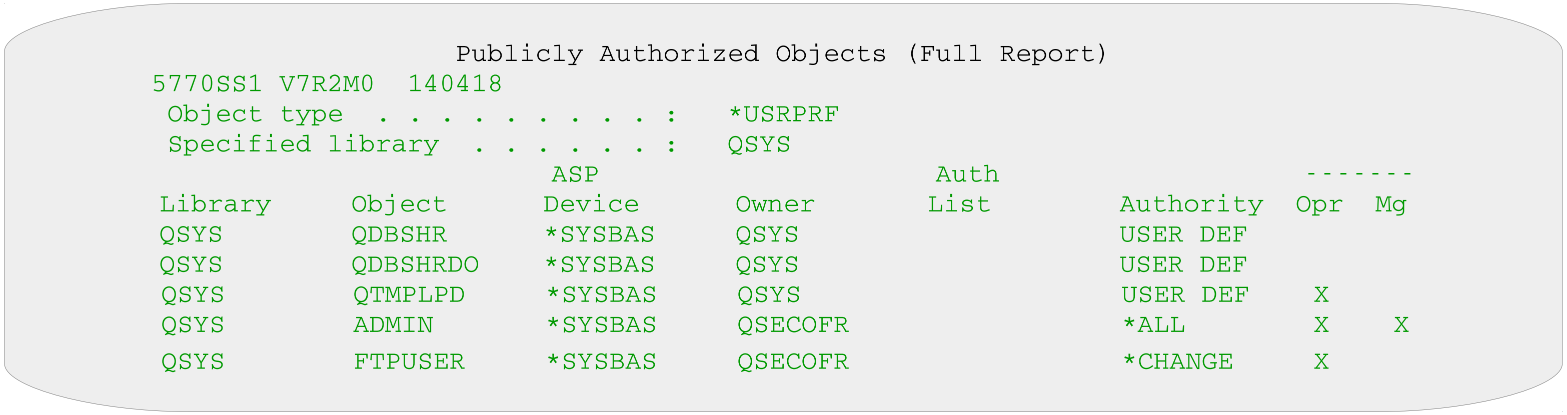
- Use password level 3 to allow passphrases, more special characters, and mixed case support

- Assign an individual password that complies with the password policies to each identified user profile

- Schedule the ANZDFTPWD ACTION(*DISABLE) command to run every night
  - Ensures that a user with a default password cannot sign on anymore

Publicly Authorized User Profiles

- Use the PRTPUBAUT OBJTYPE(*USRPRF) command to list all users with a public authority higher than *EXCLUDE



```
                  Publicly Authorized Objects (Full Report)
5770SS1 V7R2M0  140418
 Object type  . . . . . . . . . :   *USRPRF
 Specified library   . . . . . . :   QSYS
                        ASP                     Auth                  -------
Library     Object      Device      Owner       List       Authority  Opr  Mg
QSYS        QDBSHR      *SYSBAS     QSYS                   USER DEF
QSYS        QDBSHRDO    *SYSBAS     QSYS                   USER DEF
QSYS        QTMPLPD     *SYSBAS     QSYS                   USER DEF    X
QSYS        ADMIN       *SYSBAS     QSECOFR                *ALL        X    X
QSYS        FTPUSER     *SYSBAS     QSECOFR                *CHANGE     X
```

- QDBSHR, QDBSHRDO, and QTMPLPD are shipped with a higher authority
  - Authority cannot be used by others to use profiles
- Change the public authority of all (except the three IBM users) identified users back to public *EXCLUDE
  - `GRTOBJAUT OBJ(ADMIN) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)`

Unauthenticated Access via DDM

- Determine who uses DDM, typically this is BRMS and HA solutions
  - DDMACC exit program in network attributes can help

```
 System      User         User ID      PWD     Server/
  Name       Profile      on Server   Stored   RDB Name
I5OSP4       MIMIXOWN     MIMIXOWN     YES     MX_MIMIX_PDP
I5OSP4       MIMIXOWN     MIMIXOWN     YES     MX_MIMIX_SM01
I5OSP4       MIMIXOWN     MIMIXOWN     YES     MX_MIMIX_SM02
I5OSP4       QBRMS        BRMSUSER     YES     QDDMDRDASERVER
```

- Add for each user that is not already listed a server authentication entry on every system that initiates a connection:
  - Example: `ADDSVRAUTE USRPRF(QBRMS) SERVER(QDDMDRDASERVER) USRID(BRMSUSER) PASSWORD('secretpwd')`

- Once all users are added, change the DDM server attributes to require authentication. Specify at least:
  - `CHGDDMTCPA PWDRQD(*USRENCPWD)`

Unauthenticated Access via DDM (cont'd)

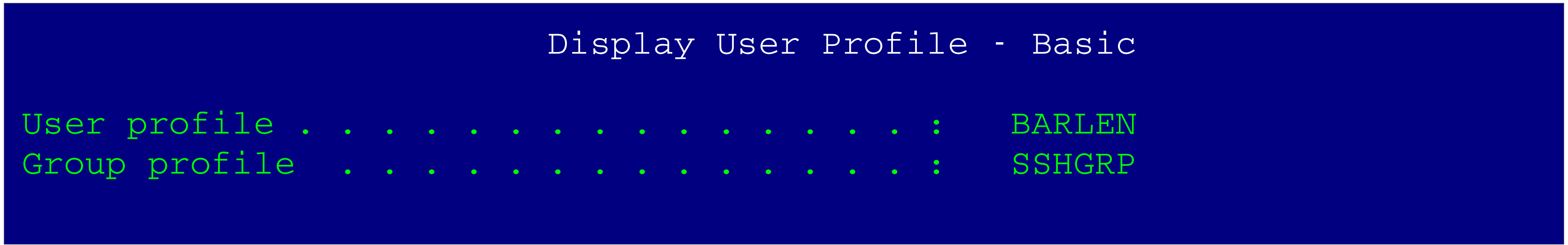
- There is an alternative to server authentication entries
- With IBM i V7R2 or higher you can use the DRDA/DDM Conjoined Mutual Authentication support to use a current user's user profile and encrypted password for authentication
  - Controlled via environment variable QIBM_CONJOINED_MUT_AUTH
  - Feature requires that
    - no server authentication entry exists for the calling user
    - no user and password is specified on the SQL connect statement
    - both systems have the same password level (QPWDLVL)

Secure shell (SSH) access

- The OpenSSH daemon runs on many systems
  - mostly used for encrypted file transfer (sftp or scp)
- The risk is that all enabled users with a valid password or configured public key authentication can connect to IBM i via ssh
  - user ends up at a PASE shell and can run shell and IBM i CL commands
    - Limited capabilities in the user profile has no effect
  - file transfer is also allowed and cannot be controlled via exit programs

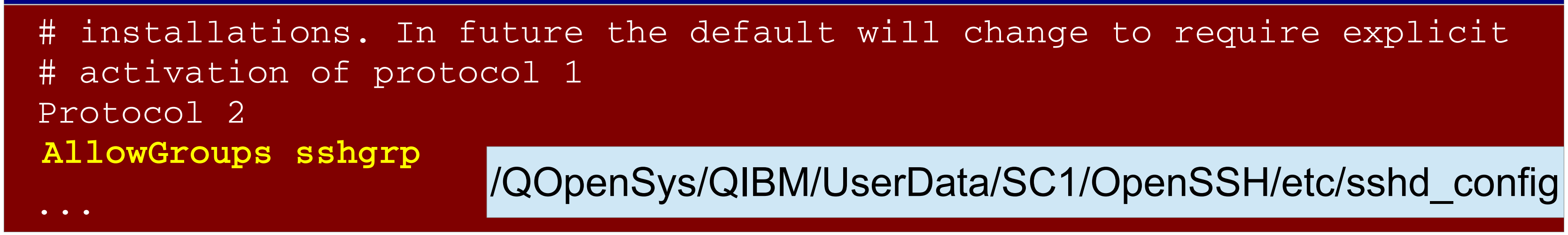
Secure shell (SSH) access (cont’d)

- Recommended to restrict SSH access
- Typically you want to permit ssh access to administrators or technical users only
- Directives exist that can deny or allow access for individual users or groups
- The order of presedence is as follows:
  - DenyUsers
  - AllowUsers
  - DenyGroups
  - AllowGroups ← best practices recommendation
- Example: Only users in group sshgrp should be able to log in via ssh



```
                         Display User Profile - Basic

User profile . . . . . . . . . . . . . . . :   BARLEN
Group profile  . . . . . . . . . . . . . . :   SSHGRP
```



```
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2
AllowGroups sshgrp
...
```

/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config

Special authorities

- Special authorities are called special because they grant high privileges to users
- All 8 special authorities in IBM i can be considered a risk when assigned to too many users

– *ALLOBJ	Access all objects on the system
– *AUDIT	Perform auditing functions
– *IOSYSCFG	Perform network configurations (i.e. TCP/IP)
– *JOBCTL	Control jobs other than the own ones
– *SAVSYS	Perform save, restore, and free strorage operations
– *SECADM	Security administrator, user management
– *SERVICE	Perform service functions
– *SPLCTL	Spool control for ALL job queues and output queues

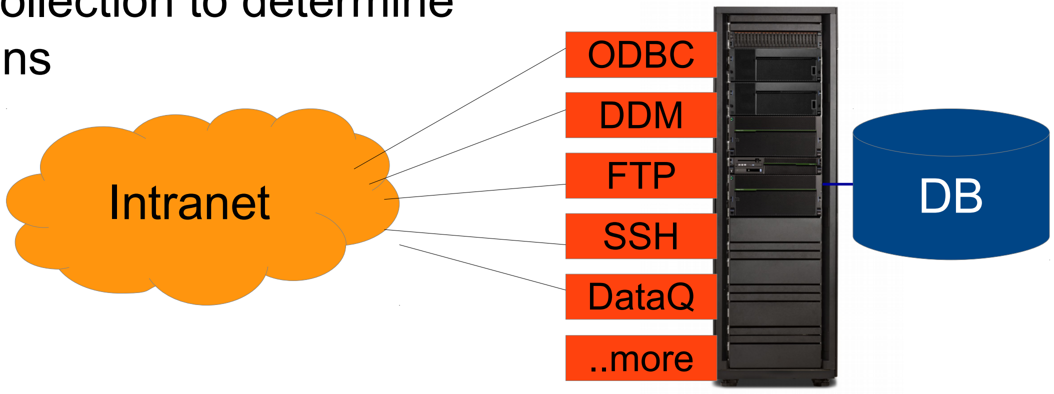
Special authorities (cont’d)

- Recommended to grant special authorities via group profiles (roles)
- Refrain from generally granting *SECOFR class special authorities
- Use wrapper programs with adopted authorities to allow certain privileged actions
- For output queues use the Display Any File (DSPDTA), Operator Controlled (OPRCTL), and Authority to Check (AUTCHK) parameter in combination with output queue object permissions to grant access to a group of users
  - Example:
    Users who are members of a group can view, copy, and control all spool files in an output queue

Object	**Parameter/Authority**	**Value**
Output queue (OUTQ)	Public authority	*EXCLUDE
Output queue (OUTQ)	User- / Group authority	*CHANGE
Output queue (OUTQ)	Display data (DSPDTA)	*YES
Output queue (OUTQ)	Operator controlled (OPRCTL)	*YES
Output queue (OUTQ)	Authority check (AUTCHK)	*DTAAUT

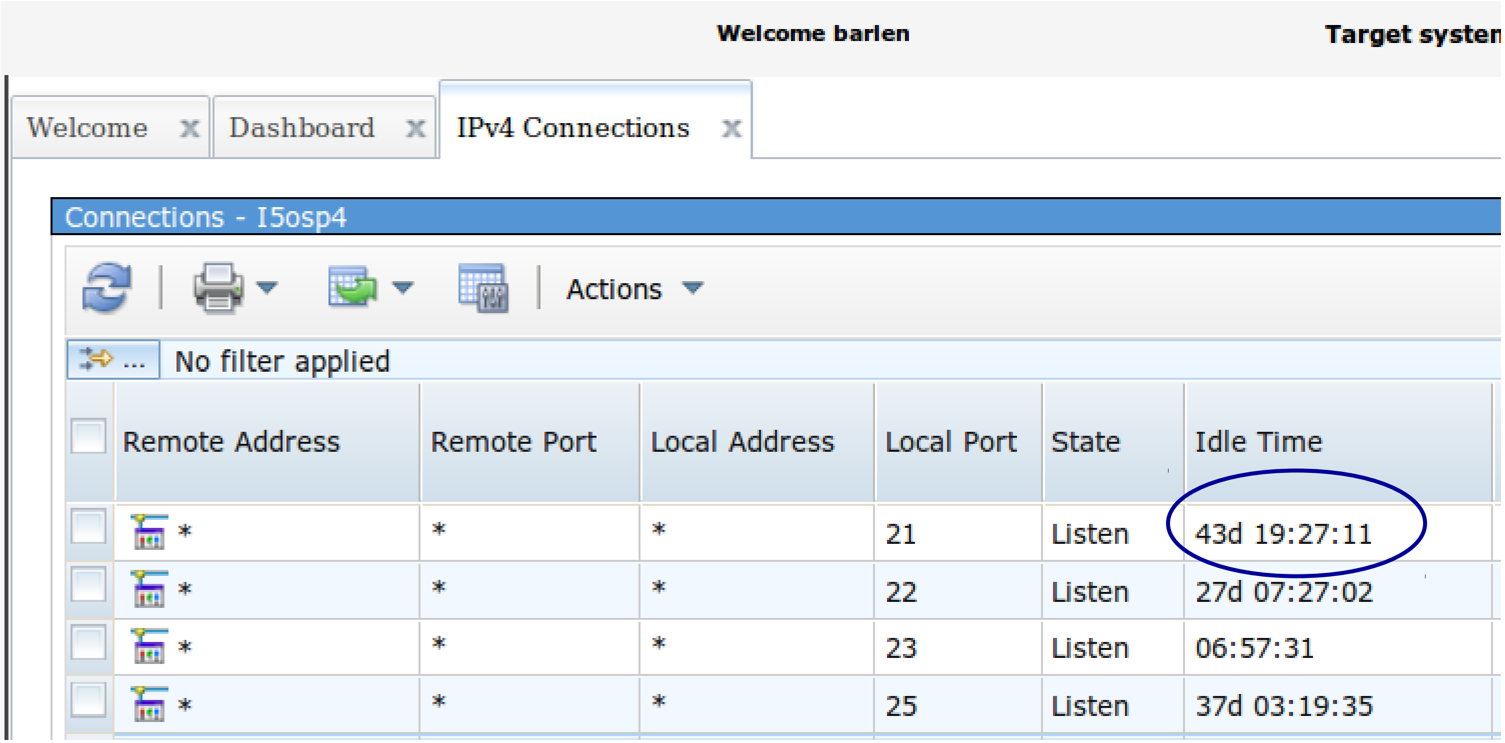
Public object authorities

- All executable code, such as program (*PGM), modules (*MODULE), commands (*CMD) should have a maximum of public *USE
  - Executable code on a production system should never have more than public *USE
- No library should have a public authority higher than *USE
- IFS directories should have a maximum of public *RX
  - Never share the IFS root
  - Share in *Read only mode whenever possible
- If an application is not written to use adopted authorities and public access to objects, such as database tables grant *USE or even higher authorities (*CHANGE or even *ALL) you should use exit point tools to tightly control access via the network
- With V7R3 use authority collection to determine required access permissions



Unused and misconfigured network services

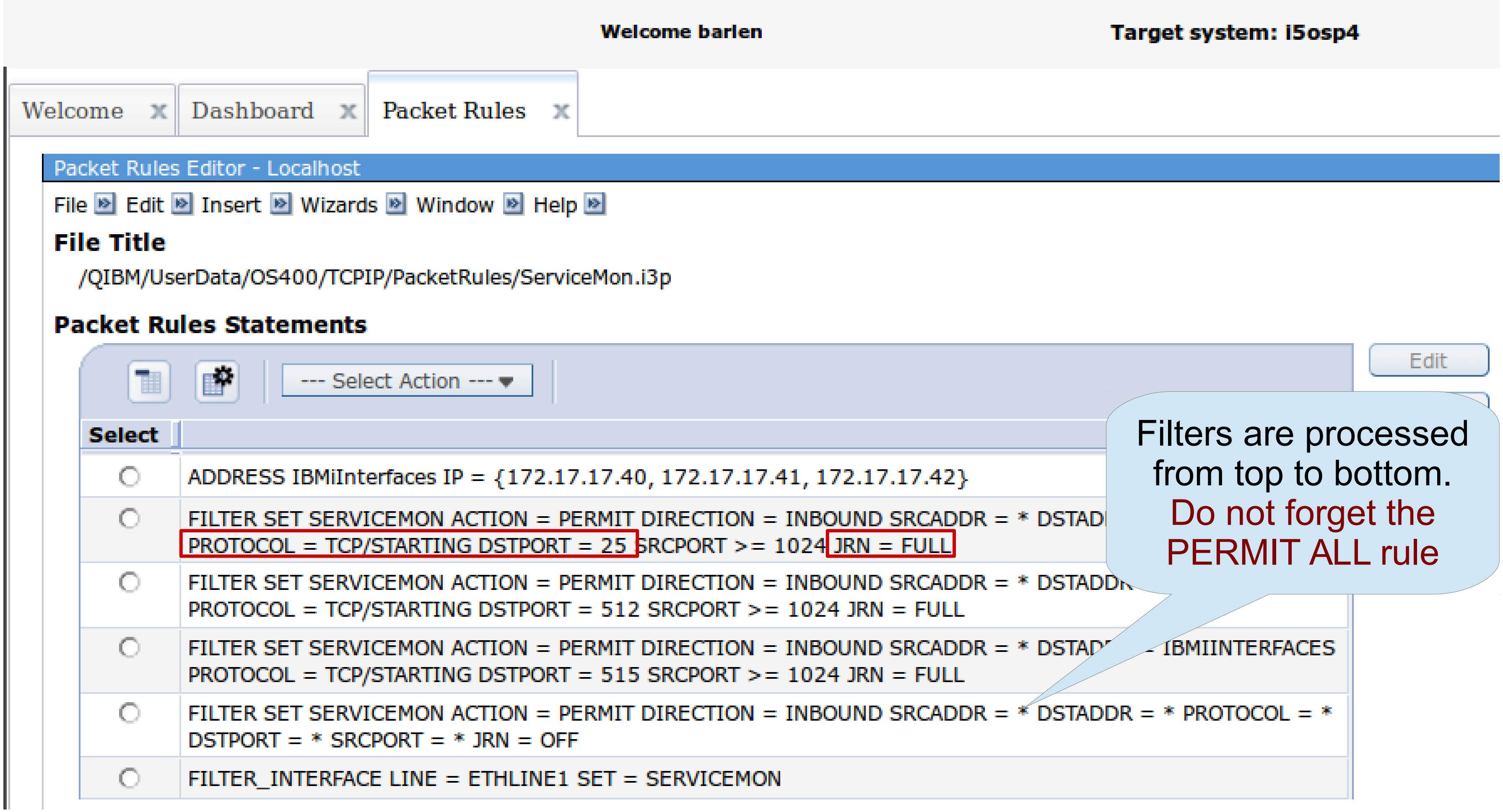
- Every network service that is not being used is a potential candidate for at least a denial-of-service attack
- Use the idle time timer in the NETSTAT *CNN display or equivalent navigator interface to determine if a network service, such as LPD or REXEC, is still being used
  - If the service has not been used since the last IPL, stop the service



□	Remote Address	Remote Port	Local Address	Local Port	State	Idle Time
□	*	*	*	21	Listen	43d 19:27:11
□	*	*	*	22	Listen	27d 07:27:02
□	*	*	*	23	Listen	06:57:31
□	*	*	*	25	Listen	37d 03:19:35

Unused and misconfigured network services (cont'd)

- IP Packet Filtering is also a good choice for determining if a network service is still being used



File Title

/QIBM/UserData/OS400/TCPIP/PacketRules/ServiceMon.i3p

Packet Rules Statements

Select	
○	ADDRESS IBMiInterfaces IP = {172.17.17.40, 172.17.17.41, 172.17.17.42}
○	FILTER SET SERVICEMON ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADI PROTOCOL = TCP/STARTING DSTPORT = 25 SRCPORT >= 1024 JRN = FULL
○	FILTER SET SERVICEMON ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR PROTOCOL = TCP/STARTING DSTPORT = 512 SRCPORT >= 1024 JRN = FULL
○	FILTER SET SERVICEMON ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTAD = IBMIINTERFACES PROTOCOL = TCP/STARTING DSTPORT = 515 SRCPORT >= 1024 JRN = FULL
○	FILTER SET SERVICEMON ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * JRN = OFF
○	FILTER_INTERFACE LINE = ETHLINE1 SET = SERVICEMON

Filters are processed from top to bottom. Do not forget the PERMIT ALL rule

Unused and misconfigured network services (cont’d)

- Evaluate the QIPFILTER journal

```
CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE)
    TOLIB(BARLEN) NEWOBJ(IPFILT)

DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF))
    OUTPUT(*OUTFILE)OUTFILFMT(*TYPE4)
    OUTFILE(BARLEN/IPFILT) ENTDTALEN(*VARLEN *CALC)
```

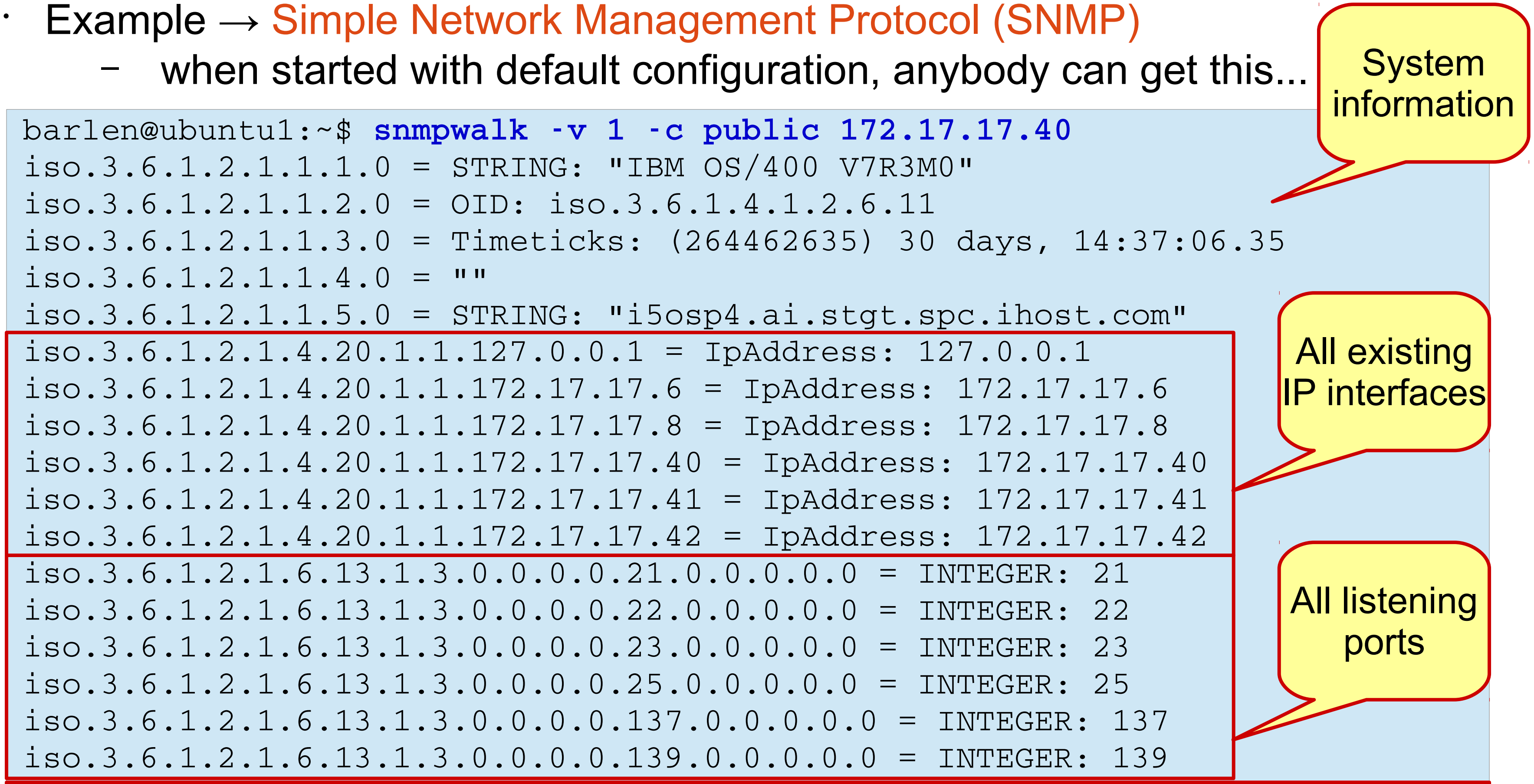
- Query the output file
  - Example shows only monitored port 25, no 512 and 515

```
LINE        FILTER ACTION  SOURCE           SOURCE  DESTINATIO        DESTINATIO
                           V4 ADDRESS       PORT    V4 ADDRESS        PORT
ETHLINE1       PERMIT      172.17.17.31     16343   172.17.17.40              25
ETHLINE1       PERMIT      172.17.8.149     41766   172.17.17.40              25
```

- When monitored over a longer period of time and port is not being used **STOP IT and change Autostart to *NO**

Unused and misconfigured network services (cont'd)

- Default configurations can also pose a risk
- Example → Simple Network Management Protocol (SNMP)
  - when started with default configuration, anybody can get this...



```
barlen@ubuntu1:~$ snmpwalk -v 1 -c public 172.17.17.40
iso.3.6.1.2.1.1.1.0 = STRING: "IBM OS/400 V7R3M0"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.2.6.11
iso.3.6.1.2.1.1.3.0 = Timeticks: (264462635) 30 days, 14:37:06.35
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "i5osp4.ai.stgt.spc.ihost.com"
iso.3.6.1.2.1.4.20.1.1.127.0.0.1 = IpAddress: 127.0.0.1
iso.3.6.1.2.1.4.20.1.1.172.17.17.6 = IpAddress: 172.17.17.6
iso.3.6.1.2.1.4.20.1.1.172.17.17.8 = IpAddress: 172.17.17.8
iso.3.6.1.2.1.4.20.1.1.172.17.17.40 = IpAddress: 172.17.17.40
iso.3.6.1.2.1.4.20.1.1.172.17.17.41 = IpAddress: 172.17.17.41
iso.3.6.1.2.1.4.20.1.1.172.17.17.42 = IpAddress: 172.17.17.42
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.21.0.0.0.0.0 = INTEGER: 21
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.22.0.0.0.0.0 = INTEGER: 22
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.23.0.0.0.0.0 = INTEGER: 23
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.25.0.0.0.0.0 = INTEGER: 25
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.137.0.0.0.0.0 = INTEGER: 137
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.139.0.0.0.0.0 = INTEGER: 139
```

System information

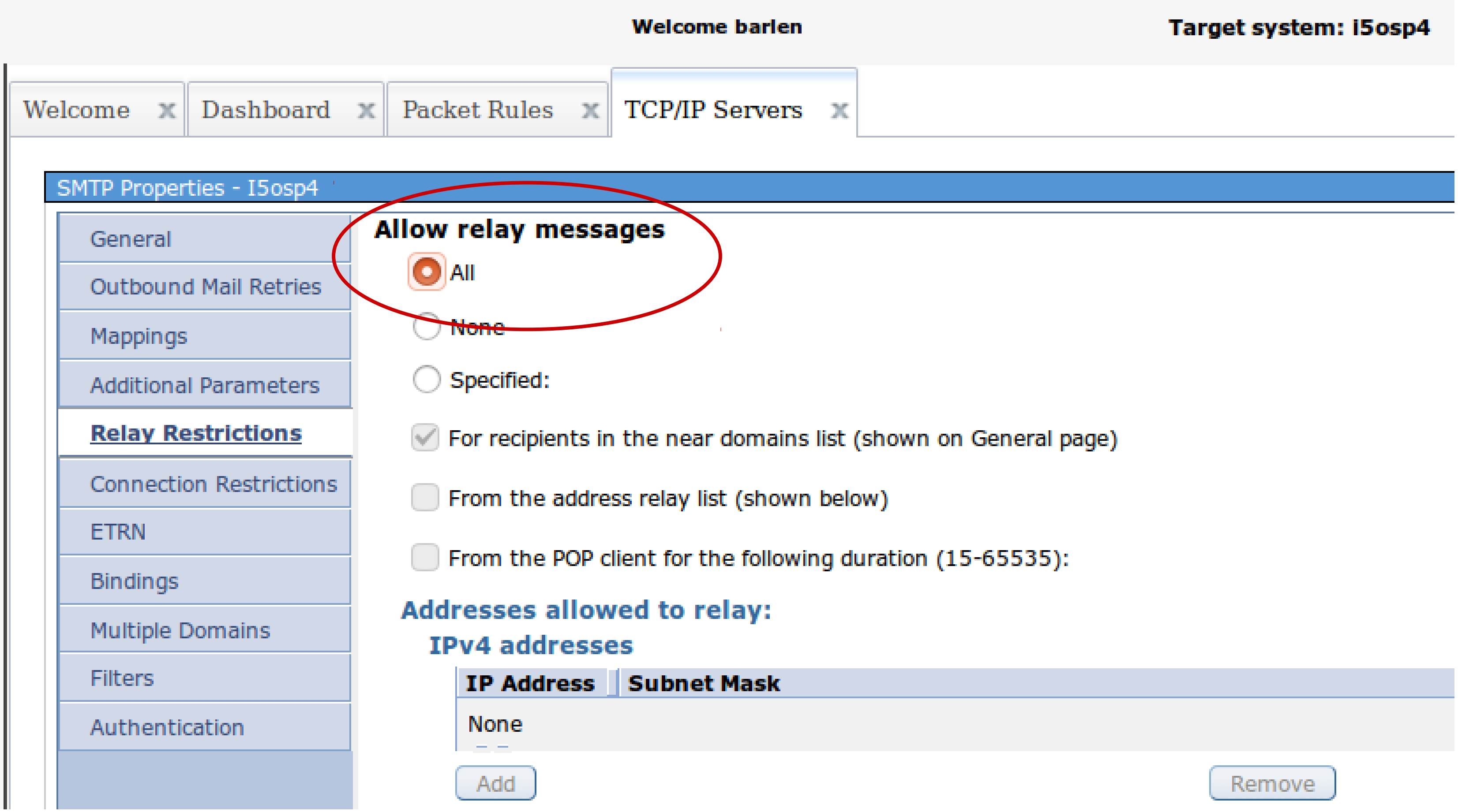
All existing IP interfaces

All listening ports

Over 2800 entries returned including installed HW, filesystem names, installed license programs, etc.

Unused and misconfigured network services (cont’d)

- Example → Simple Mail Transfer Protocol (SMTP)
  - Acts by default as an open mail relay → mail spamming



Allow relay messages

● All

○ None

○ Specified:

☑ For recipients in the near domains list (shown on General page)

☐ From the address relay list (shown below)

☐ From the POP client for the following duration (15-65535):

Addresses allowed to relay:

IPv4 addresses

IP Address	Subnet Mask
None	

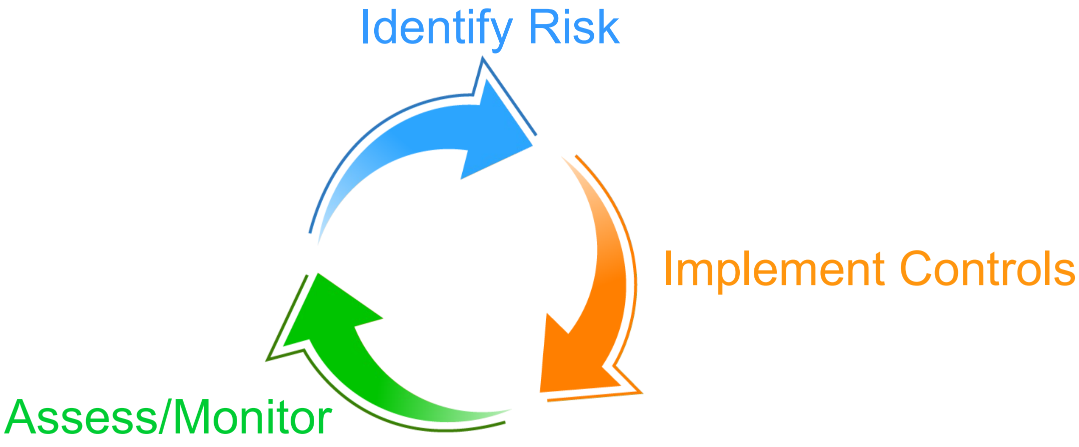
Policies

- Corporate security policies are crucial for a consistent security setup throughout the IT landscape
  - Every administrator knows what to do and what not to do

- IBM i security configurations should be thoroughly documented
  - for future reference
  - to demonstrate to auditors what have been done and why
  - configuration changes are best documented in a setup program (i.e. CL program) that runs after a new install or release upgrade

Compliance monitoring

- Audits and security assessments only provide a snapshot of the security state at a given time
- Continuous monitoring needs to be implemented to ensure
  - that no unauthorized changes are made
  - detection of security violations
  - your system is still at the desired security state
- Compliance tools can help you with automating monitoring tasks
  - various tools exist from IBM and third-party vendors



Conclusion

- Common findings during a security assessment
  - Default passwords
  - Publicly authorized profiles
  - DDM access without authentication
  - SSH access
  - Special authorities
  - Public authorities
  - Unused network services
- Addressing identified high risks
  - Remediation
- Compliance monitoring
  - Policy definition
  - Monitoring tools

Thanks

IBM Systems Lab Services and Training

Our Mission and Profile

- Support the IBM Systems Agenda and accelerate the adoption of new products and solutions
- Maximize performance of our clients' existing IBM systems
- Deliver technical training, conferences, and other services tailored to meet client needs
- Team with IBM Service Providers to optimize the deployment of IBM solutions (GTS, GBS, SWG Lab Services and our IBM Business Partners)

Our Competitive Advantage

- Leverage relationships with the IBM development labs to build deep technical skills and exploit the expertise of our developers
- Combined expertise of Lab Services and the Training for Systems team
- Skills can be deployed worldwide to assure all client needs can be met

Want get the state of security for your IBM i environment?

- IBM Systems Lab Services offers two types of security assessments
  - 1. Remote security assessment examining the most critical areas on an IBM i partition (fixed price)
  - 2. Onsite/Offsite security assessment examining many different areas (length may vary based on environment, typical 40 hours)

IBM Systems Lab Services and Training

Our Mission and Profile

- Support the IBM Systems Agenda and accelerate the adoption of new products and solutions
- Maximize performance of our clients' existing IBM systems
- Deliver technical training, conferences, and other services tailored to meet client needs
- Team with IBM Service Providers to optimize the deployment of IBM solutions (GTS, GBS, SWG Lab Services and our IBM Business Partners)

Our Competitive Advantage

- Leverage relationships with the IBM development labs to build deep technical skills and exploit the expertise of our developers
- Combined expertise of Lab Services and the Training for Systems team
- Skills can be deployed worldwide to assure all client needs can be met
- Contact: Beatrice Coulomb (bcoulomb@fr.ibm.com) or Claude Roustan (claude.roustan@fr.ibm.com)