PowerTech
SECURITY SCAN

08.29.17

Thank you for using PowerTech Security scan and taking the first step to ensure security for your IBM i (System i®, iSeries®, AS/400®). You will find summary of results along with detailed information. The scan results will provide helpful information about what is at risk and how to improve security.

Learn how to keep your system safe with these PowerTech solutions:

- Authority Broker
- Command Security
- Compliance Monitor
- DataThread
- Interact
- Network Security
- Policy Minder
- PowerAdmin
- RSA Secure ID
- Password Self Help
- StandGuard Anti-Virus

Be sure to check out the PowerTech Online Compliance Guide which provides in-depth information on each topic plus recommendations on how to configure and audit your systems to comply with regulations like HIPAA and PCI.

*This report contains hyperlinks to PowerTechs online Compliance Guide, which provides in-depth information on each topic plus recommendations on how to configure and audit your systems to comply with regulations like HIPAA and PCI.

SYSTEM INFORMATION

System Name: SAMPLE

Report Date: 03/04/2015

Model: 42A

Type: 8286-EPXF

LPAR: 7

PGroup: P20

Version: V7R2M0

CCSID: 00037

SUMMARY

Security Breach Risk

HIGH

The majority of IBM i servers today are open to vulnerabilities unique to the IBM i architecture and the applications on the system.

What is COBIT?

This Security Scan reviews security vulnerabilities in six major categories and maps them to corresponding COBIT controls.

COBIT is a control framework for Information Technology best practices that many auditing firms use as a guide to assess compliance with Sarbanes Oxley (SOX) and other regulations.

Security Scan Results

1 Admin Privileges

AI 3.2 - Infrastructure Resource Protection

DS 5.3 - Identity Management

2 Public Authority

DS 5.4 - User Account Management

3 Network Access

DS 5.3 - Identity Management

DS 5.5 - Security Testing, Surveillance, and Monitoring

4 FTP Access

Overall risk level and general information regarding ftp access

5 System Security

DS 5.9 - System Security

6 User Security

DS 5.3 - Identity Management

DS 5.4 - User Account Management

7 System Auditing

DS 5.5 - Security Testing, Surveillance, and Monitoring

Software Tools That Monitor

Even experienced IT security personnel need quality software tools to monitor, detect, and block security breaches. An enormous number of business transactions occur on your system daily and any of them may be important to your security. A typical IBM i user generates between 50 and 300 security-related audit events each day.

Your User ID Count

68

Transactions per Day

3,400 - 20,400

Your system has 68 user IDs, which translates into 3,400 to 20,400 transactions per day. As end users become more sophisticated, the number of security events increases, making it more difficult to detect security breaches.

1 ADMIN PRIVILEGES

Admin Privileges Risk

MEDIUM RISK

Administrative Privileges are called Special Authorities. These rights are very powerful and should be for trusted and knowledgeable IT professionals only. Users with these special authorities should have their activities audited.

Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated. IBM i servers typically run mission-critical applications, and special authorities grant users special privileges for these components.

Relevant COBIT objectives

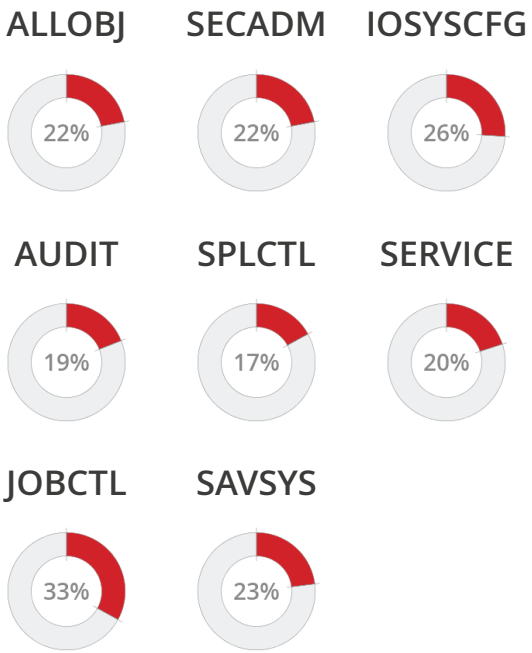
- COBIT DS5.3: - Identity Management
- COBIT DS5.4: - User Account Management
- COBIT AI3.2: - Infrastructure Resource Protection and Availability

*ALLOBJ special authority

A developer, programmer, or database administrator with *ALLOBJ special authority on a production system has full access to make changes to sensitive information in databases. Segregation of duties cannot be enforced if the IT staff have special privileges in their everyday business profiles.

Recommended threshold of users with each special authority:

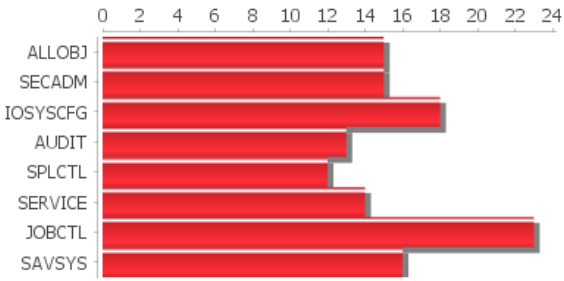
These are the percentage of the users with each special authority:



Special authorities above the recommended threshold:

8 OF 8

These are the users with each special authority:



2 PUBLIC AUTHORITY

Public Authority to Libraries

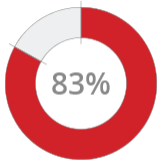
LOW RISK

IBM i is shipped with a default set of permissions assigned to the general user population (*PUBLIC).

*PUBLIC access to libraries is a measurement that indicates how accessible the system is to the average end user. As defined by the operating system, *PUBLIC represents any user that can log in and that has no explicit authority.

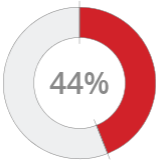
Learn more about how to monitor and audit library authority settings in the PowerTech Compliance Guide

*Public rights



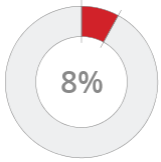
All users (*PUBLIC) that have the rights to read or change libraries on this system.

*CHANGE



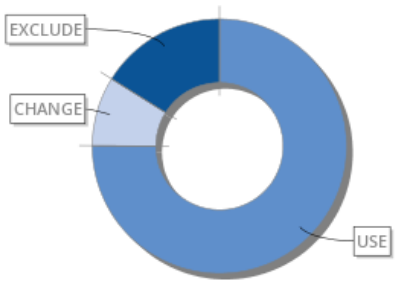
Public receives "*CHANGE" on newly created objects in 30 libraries.

Deleting data



All users can delete data or applications from more than 6 of the libraries.

Public permissions in libraries



Authority	Libraries	Percentage
USE	51	75.0
CHANGE	6	8.8
ALL	0	0.0
AUTL	0	0.0
USER DEF	0	0.0
Read and oper	0	0.0
EXCLUDE	11	16.1

Total number of libraries on this system: 68

Learn more about how to monitor and audit library authority settings in the PowerTech Compliance Guide

3 NETWORK ACCESS

Security of Network Access

Security of user access across the network is at risk on this system. The IBM i is shipped with a variety of network services that are factory configured and ready to communicate with other computers. All IBM i servers should have exit programs on IBM network servers to monitor and control network access.

Relevant COBIT objectives

COBITDS5.3 : Identity Management

Ensure that all users (internal, external, and temporary) and their activity on IT systems (business application, system operation, development, and maintenance) are uniquely identifiable.

COBITDS5.5 : Security, Testing, Surveillance, and Monitoring

Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed. Learn more in PowerTech Compliance Guide

Most visible network services are

FTP

The FTP server can upload data Ffrom a PC to the System IBM i and download data to a PC. Any user with a PC can perform the common FTP commands like list directories, change directories, put (upload) files, get (download) files, and delete files.

Exposure!
- On SAMPLE, FTP activity is not being monitored by exit programs and there are no access control rules in place to prevent users from transferring critical data over FTP.

Database

ODBC database connections can manipulate information in database files on the System IBM i using common SQL commands like UPDATE, SELECT, DELETE. Most PCs have ODBC drivers installed that allow users to access data directly on System IBM i servers. Often, it's as easy as selecting a drop-down menu in Microsoft Excel.

Exposure!
- On SAMPLE, the database server is not being monitored by exit programs and there are no access control rules in place to prevent users from manipulating critical data via ODBC connections.

Remote Command

Any user on a PC with IBM's Client Access can issue commands remotely to an System IBM i server that they connect to through the network. The limit capability setting on their user profile does not affect their ability to run remote commands.

Exposure!
- On SAMPLE, Remote Command activity is not being monitored by exit programs and there are no access control rules in place to prevent users from entering critical system commands from a PC.

3 NETWORK ACCESS

IBM i Exit Programs in Place

Network programs not in place

DDM

Distributed Data Management (DDM) is an IBM protocol that provides users, or applications, with remote access to database files. DDM access to this system is not secured.

Command Line Access

There are 62 user profiles on this system with command line access, 59 of which are enabled.

If a user has command line authority (LMTCPB *NO or *PARTIAL), they can run virtually any of the more than 2000 commands that are shipped with the operating system. Some of these commands, such as DSPJOB and DSPLIB, are not of great concern. Others, such as ENDJOB, ENDSBS, and DLTJOB are of greater concern, especially if the underlying objects are not properly secured. If a user has access to a command line, the number of things they can do is often limitless. You can use the LMTCPB attribute of a user profile to limit the command line access of users.

Most visible network services are:

	Exit Point Server	Description	Exit Program	Importance
1	*FILESRV	Remote File Server - Used when drives are mapped to IFS	✗	HIGH
2	*TFRFCL	Client File Transfer Server	✗	HIGH
3	*FTPSERVER	File Transfer Protocol (FTP) server on the System i	✗	HIGH
4	*FTPREXEC	Remote command thru FTP	✗	HIGH
5	*REXEC_SO	Remote Command Sign-on (log on)	✗	HIGH
6	*SQL	ODBC & JDBC Sign on (log on)	✗	HIGH
7	*NDB	ODBC & JDBC Native Database	✗	HIGH
8	*RTVOBJINF	ODBC & JDBC Retrieve Object Info	✗	HIGH
9	*SQLSRV 1	ODBC & JDBC Server	✗	HIGH
10	*SQLSRV 2	ODBC & JDBC Server	✗	HIGH
11	*RMTSRV	Remote Command Server	✗	HIGH

3 NETWORK ACCESS

	Exit Point Server	Description	Exit Program	Importance
12	*DQSRV	Client Data Queue Server	✖	MEDIUM
13	*TELNET	TCP/IP Terminal Emulation	✖	MEDIUM
14	*FTPCLIENT	File Transfer Protocol (FTP) client on the System i	✖	MEDIUM
15	*TFTP	Trivial FTP	✖	MEDIUM
16	*DATAQSRV	Remote Data Queue Server	✖	MEDIUM
17	*LMSRV	Client License Server	✖	LOW
18	*MSGFCL	Client Message Server	✖	LOW
19	*QNPSERVR	Virtual Print Server : (Entry)	✖	LOW
20	*QNPSERVR	Virtual Print Server : (Spool File)	✖	LOW
21	*RQSRV	Client Remote SQL Server	✖	LOW
22	*FTPSIGNON 1	Allow/Prevent Anonymous FTP	✖	LOW
23	*VPRT	Client Virtual Print Server	✖	LOW
24	*CNTRLSRV	Client Access License Server: (License Mgt)	✖	LOW
25	*CNTRLSRV	Client Access License Server: (Conversion Map)	✖	LOW
26	*CNTRLSRV	Client Access License Server: (Client Mgt)	✖	LOW
27	*SIGNON	OS/400 Signon Server	✖	LOW

4 FTP ACCESS

FTP Access on This System

HIGH RISK

FTP is an industry-standard client/server protocol widely used for performing file transfers between two devices. IBM i has the ability to act as client and/or server. While convenient and fast, FTP enables a user to access objects (including data files) for which they have object-level permission or, if a profile has *ALLOBJ special authority, any object on the server. FTP represents a significant risk to any server that has no security configured, or that relies on legacy restrictions such as menus and limited capabilities.

FTP Popularity

Despite its continued prevalence in many IBM i environments, FTP has lost popularity with security professionals because data transfers occur without encryption, making the protocol insecure.

On this system, the FTP server is currently configured to automatically start. That does not necessarily mean it is currently running, but it is configured to start automatically after the next IPL. There is also nothing to prevent one of the 18 users with *IOSYSCFG special authority from starting it on demand.

Total number of user profiles with potential FTP access

HelpSystems recommends the following solutions to take advantage of preventing access with secure transmission protocols:

Exit Programs

We recommended an exit program in order to prevent unauthorized access regardless of whether the server is started or not. An exit program can also provide oversight of user requests as well as detection of brute force attacks against this commonly-attacked entry point. For more information on this, see the NETWORK ACCESS section.

FTPS

FTPS is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. Migrating from FTP to FTPS is straightforward and it will encrypt all file transfers and user credentials in transit.

4 FTP ACCESS

SFTP

SFTP (SSH File Transfer Protocol) is one of the most widely used and secure file transfer protocols to exchange data. It is easier to setup and administrate compared to FTP or FTPS since it only requires a single open firewall port. And, with additional authentication options using an SSH key in addition to a password (or in lieu of it), SFTP is the clear choice for many organizations.

HTTPS

HTTPS is most commonly known for accessing websites from popular internet browsers, but this secure protocol is also ideal for transferring files using an API or web service interface like SOAP and REST.

User native search commands and integration of native FTP

FTP and native server commands

FTP supports the ability for a user to issue native server commands as an alternative to the native command line. In some cases, a user can execute commands despite having a Limited Capabilities (LMTCPB) setting of *YES specified on their profile. An example is the Delete Library (DLTLIB) command. This can represent major risk if the expectation is that the user has no access to a command line in the native environment.

Integration of Native FTP

Thanks to the integration of native FTP within the IBM i operating system, data transfer functionality and command execution is accessed by a user logging in with the same credentials used for native 5250 access. This can result in unexpected data loss and even server and data corruption by users that are not trained and have no explicit business need. Unfortunately, FTP on IBM i does not contain an activity log, rendering most user activities invisible. This is a common audit violation.

5 SYSTEM SECURITY

System Security

The operating system provides a number of methods of securing itself and the workstations connected to it. In this section we examine the system values that protect your operating system and your workstations.

Relevant COBIT objectives

COBIT DS5.9: Malicious Software Prevention, Detection, and Correction

Put preventive, detective, and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

Learn more about User Security and Password Settings in the PowerTech Compliance Guide

System values that protect your operating system and your workstations:

System Value	Comments	Value	Ratings
QSECURITY	Your system is running at level 40 (QSECURITY), the minimum setting recommended by IBM.	40	GOOD
QALWOBJRST	There are no restrictions on the types of programs that can be loaded on this system. A knowledgeable programmer (including a vendor or a contractor) could load programs that bypass your security without being detected.	*ALL	WEAK
QVFYOBJRST	Programs are not checked for valid signatures when loaded on this system. The source and authenticity of operating system programs cannot be validated by this system.	1	WEAK
QUSEADPAUT	Any system user could create programs that adopt another user's authority.	*NONE	WEAK
QDEVRCYACN	Jobs that experience a communications failure are ended automatically.	*DSCMSG	GOOD
QINACTITV	Interactive jobs on this system never time out for lack of use.	*NONE	WEAK
QLMTDEVSSN	There is no limit to the number of concurrent sessions a user can start.	0	MODERATE
QLMTSECOFR	There is no limit to which workstations a security officer can sign on to.	0	MODERATE
QMAXSIGN	Users are permitted 5 attempts to sign on before an action is taken.	5	MODERATE
QMAXSGNACN	Workstation is disabled.	1	MODERATE

5 SYSTEM SECURITY

Anti-virus

Correct settings for the system values in this category help ensure that no inappropriate or malicious software is installed on the system.

System Value	Comments	Value	Ratings
QSCANFS	Stream files in the root(/), QOpenSys, and user-defined file systems will be scanned for virus threats.	*ROOTOPNUD	GOOD
QSCANFSCTL	All accesses will be scanned which may degrade system or application performance.	*NONE	MODERATE

You have no virus scanning enabled when a file is opened.

You have no virus scanning enabled when a file is closed.

6 USER SECURITY

User Security and Passwords

User and password security are critical because they are the easiest way to compromise a system. On this system the security controls for users and passwords have been scanned with the listed results.

IBM password policy recommendations

The ISO 27002 requirements

These are the recommendations for the password policy based on IBM recommendations and the ISO 27002 (formerly known as 17799) standard, which provides detailed guidance for setting strong password policies and managing user accounts. COBIT points out the need for effective management of user accounts.

COBIT DS5.3: Identity Management

Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, system operation, development, and maintenance) are uniquely identifiable.

COBIT DS5.4: User Account Management

Address requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges.

The following information is an overview to outline your user and password security:

User Security

The 2 areas are a high degree of concern:

Category	Recommendations	SAMPLE
Inactive User ID	0	✖3(3 Enabled)
Number of Users with Invalid Sign on Attempts	Less than 5	✔0
Largest number of Invalid Sign on Attempts on 1 profile	Less than 3	✔0
Unsecured User Profiles	0	✔0
Users with Default Passwords	0	✖7(6 Enabled)

Password Settings

The Password Settings table shows that password rules are weak on this system.

Password Settings	Standard	SAMPLE
Expiration	90 Days	✖*NONE
Minimum Length	6 Characters	✖4 Characters
Digits Required?	Yes	✖No
Different from previous	10 Passwords	✖0 Passwords
Block Password Change	24 Hours	✖*NONE
Password Rules	Per Corporate Policy	⚠*PWDSYSVAL

Learn more about User Security and Password Settings in the PowerTech Compliance Guide

7 SYSTEM AUDITING

System Auditing Features

A major feature of the operating system is its ability to log important, security-related events in a secure audit journal.

- System auditing is not turned on.
- The Security log (QAUDJRN) does not exist on SAMPLE.

The default value for auditing of new objects is to not audit objects. (QCRTOBJAUD)

Logging data and audit tools are not being used.

Logging Data	Audit Tools
✖	✖

Auditing Network Events: The operating system provides multiple exit points that enable the monitoring of make it possible to monitor network traffic due to popular services such as FTP, ODBC, and DDM.

You can review which exit points are monitored on the Network Access section.

Audit Value	Description	Value	Importance
*AUTFAIL	Log authority failures	✖	HIGH
*CREATE	Log creation of new objects	✖	HIGH
*DELETE	Log deletion of objects	✖	HIGH
*PGMFAIL	Log program failures caused by security violations	✖	HIGH
*PTFOPR	Log PTF operations	✖	HIGH
*SAVRST	Log restore actions to security sensitive objects	✖	HIGH
*SECURITY	Log security related changes	✖	HIGH
*SERVICE	Log usage of the system and hardware service tools	✖	HIGH
*JOBDTA	Log job events such as start and stop	✖	MEDIUM
*OBJMGT	Log object management changes	✖	MEDIUM
*PGMADP	Log usage of programs that adopt authority	✖	MEDIUM
*PTFOBJ	Log changes to PTF objects	✖	MEDIUM
*SYSMGT	Log changes to certain system management areas	✖	MEDIUM
*NETCMN	Log APPN firewall events	✖	LOW
*NETSCK	Log socket tasks	✖	LOW
*NETSECURE	Log secure network connections	✖	LOW

7 SYSTEM AUDITING

Audit Value	Description	Value	Importance
*NETTELSVR	Log TELNET server connections	✖	LOW
*NETUDP	Log User Datagram Protocol (UDP) traffic	✖	LOW
*OFCSRV	Log Office Vision/400 security changes	✖	LOW
*OPTICAL	Log of usage of optical storage devices	✖	LOW
*PRTDTA	Log of printing functions	✖	LOW
*SPLFDTA	Log usage of spooled files (reports)	✖	LOW

RECOMMENDATIONS

Recommendations for System

These recommendations come from compliance checks performed on the system. Using that information, the recommendations were created in priority order, based on three factors: security risk, time to complete, and estimated cost.

1 Admin Rights Recommendations

Administrative Rights: - Special Authority -- All of these Special Authorities should be reviewed and the number of profiles for each should be reduced to the minimum. The rationale for granting these special authorities should be documented. Once the standards are set, start regular monitoring regularly so that any new special authorities are highlighted.

PowerTech Authority Brokerenables companies organizations to cut down on the number of user profiles with special authorities. Users swap to increased privilege levels only when it is necessary and their actions are audited.

3 User Access Recommendations

Secure and Monitor Network Transactions Immediately - This System i server is open to any PC on your network through a variety of network-enabled services. PC-to-System i transactions are untraceable and uncontrollable on these servers. This type of network access is the greatest weakness in your current system implementation. We strongly recommend that you control and monitor network activity to and from your System i servers. Currently, any user with a PC and valid Uuser ID can access all of the data on the system through network services and bypass your menu security.

PowerTech Network Securityis a leading access control solution for the System i that lets you monitor and control network access through exit points.

6 User Security Recommendations

Implement Standards for User Security - This server does not have consistent standards. We made recommendations based on industry experience and standards. In some cases, you may need to deviate from the industry standard. In those cases, we recommend documenting each deviation.

Inactive Profiles - Monitor for inactive User IDs and remove them from the system. Eliminate the 3 inactive profiles (3 are enabled) on this system.

Profiles with Default Passwords - 7 profiles have default passwords (6 are enabled). Reduce this number to zero and monitor for new ones.

7 System Auditing Recommendations

Set Security Event Trigger Points - This system could log thousands of security events daily, but there is no way to sort and filter the important events and notify the right people. Also, the operating system does not provide a way to track TCP/IP traffic, such as ODBC or FTP, to the system. Implement a System i security/auditing solution that tells you: Who has authority to what? What events are security exposures? What new exposures are being created daily?

PowerTech Compliance Monitor allows you to automatically generate customized audit reports on a regular basis for each customer.