IBM i Security Assessment and Advisory Report

System: 1.1.1.105 **Version:** V5R3 **QSECURITY:** 40
Processor: 7459 **Model:** 520 **Serial Number:** 44DE466

Sunday, July 20, 2014, 9:35 AM

Table Of Contents

1. About This Assessment

Raz-Lee Security Assessment

Raz-Lee Security is proud to provide you with this free security assessment report for your IBM i.

This security assessment report was designed, reviewed and carefully tested by experienced security professionals with indepth knowledge of all aspects of IBM i security. Their certification for this assessment report appears below.

Disclaimer: It is important to emphasize that with the inevitable differences between IBM i implementation and configurations, the Security Assessment results and recommendations should only be implemented by trained professionals, following careful examination of their potential implications to the company's specific requirements, policies and procedures.

For the full information

1.1 About Raz-Lee

Raz-Lee Security (www.razlee.com) is the developer of iSecurity™, the leading security solution for the IBM i (AS/400). Founded in 1983, Raz-Lee Security Inc. has leveraged its years of experience to design, develop and market comprehensive security solutions, exclusively customized to assure maximum system protection. With iSecurity™, Raz-Lee sets the new IBM i security standard in the market.

iSecurity™ provides users with SOX (Sarbanes-Oxley), HIPAA, Basel and other leading market standards and requirements. Raz-Lee Security Inc. provides a leadership role in the evolution of IBM i security solutions, from innovative technology to cutting-edge solutions. iSecurity™ protects the organization's entire data and assures successful business continuity.

Raz-Lee continues its commitment and dedication to providing today's cutting-edge security solutions and technology for the IBM i environment. Raz-Lee is constantly striving to bring innovative IBM i security solutions to the market.

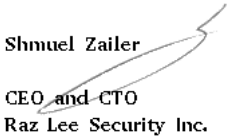
1.2 Certificate 2010

We, the undersigned, have reviewed the design and validated the recommendations of this security assessment and advisory system.

As experienced IBM i security developers, we certify that the results of this assessment properly represent the security level in all evaluated areas.

We are certain that this evaluation will provide tangible value for management, system administrators and security advisors.

The importance given to each line item, the setting of the rules for the scoring and the advice provided are our personal opinion and should only be considered as such.



Shmuel Zailer

CEO and CTO
Raz Lee Security Inc.

Eli Hilleli

iSeries Security Consultant
Aviv Systems

About Shmuel Zailer

Mr. Shmuel Zailer, Raz-Lee Security's CEO and CTO, is a world-renowned expert in IBM i software technology, having successfully developed, sold and marketed AS/400-related optimization and performance software products including IBM i security solutions, for the past 24 years. He also served as the leading security consultant to multi-national companies worldwide.

About Eli Hilleli

Mr. Eli Hilleli is an IBM i security expert with more than 20 years of experience in AS/400 systems management, administration and programming, specializing in security and performance issues.

To print the certificate

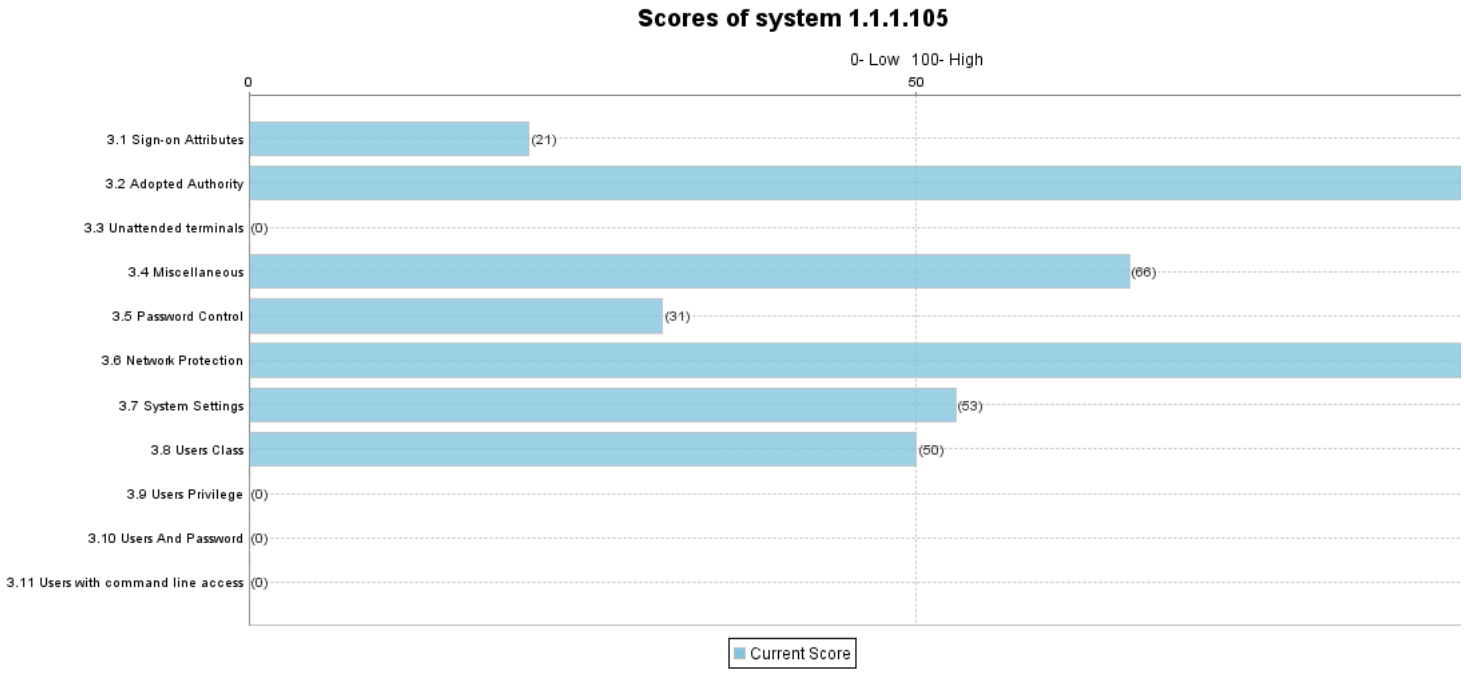
Note: We strongly recommend printing the assessment report using "landscape" rather than "portrait" orientation..

2. Executive Summary

A proper and thorough security policy can only be implemented after assessing the strengths and weaknesses of the System i. Your System i 1.1.1.105 underwent comprehensive security checks in order to assist you in evaluating and implementing optimal security measures for this system. This security assessment report was generated on Sunday, July 20, 2014 9:35 AM system time.

This assessment report is structured as follows: for each subject in the Detailed Analysis Section (section 3) a table is presented listing, for each system value, exit point, etc. its descriptive components as well as the current value of the item, our expert's recommended value, the "Current Score" of this item, and finally the overall "Current Score" of this section, the "Score with iSecurity", i.e. the score attainable using iSecurity, and a short summary explanation of your security status for this section.

Should you have any questions, feel free to contact us. Contact Details appear in Section 4 below.



* * *

Final Score : ★☆☆☆☆

Explanation: Total computer scores reveal several flaws in the system. The System Administrator should immediately revise the computer's security policies or risk facing a possible security threat.

* * *

Section	Score	Explanation
3.1 Sign-on Attributes	21	The computer's settings are invalid and pose immediate security threats. **iSecurity User Sign On functionality should be implemented.**
3.2 Use of Adopted Authority	100	The computer's Adopted Authority security is perfect; the System Administrator can control who creates such programs but cannot review program usage.
3.3 Unattended terminals	0	Computer settings are faulty. **Avoid a possible security threat to the network by implementing iSecurity Screen.**
3.4 Miscellaneous Sign-on	66	Some miscellaneous sign-on values are in accordance with industry standards. However, the computer's scores are borderline and should be reviewed.
3.5 Password Control	31	Computer settings are faulty and open to password-related security threats. **iSecurity Password should be implemented.**
3.6 Activation of Network Protection	82	Most of the computer's exit points are protected; minor revisions will enable the computer to be fully protected. **iSecurity Firewall is the only product on the market which controls and manages all security-related IBM i exit points and is required in a PC-emulated environment.**
3.7 Auditing System and User Activities	53	Most of the computer's auditing policies are not in place and therefore pose a possible security threat. **iSecurity Audit should be implemented.**
3.8 Users Class	50	This number is too high for proper security; review security policies and reduce the number of power users. **iSecurity Audit should be implemented.**
3.9 Analyzing Users By Privilege	0	Since you have greatly exceeded the number of recommended privileged users, enterprise data is far too easily accessible. The System Administrator should reduce that number immediately. **iSecurity Audit should be implemented to manage and possibly disable all network access, and especially activities generated from users having All Object Authority.**
3.10 Users with default password	0	The number of enabled users with a default password is much too high and poses a serious security risk. **Reduce the number of enabled users and implement iSecurity Password.**
3.11 Users with command line access	0	This number is too high and poses a security risk. **Reduce the number of users with command line access.**

Legend		
High risk	Medium risk	Low risk

Top

* * * * *

3. Detailed Analysis:

3.1 Sign-on Attributes

Sign-on is the gateway to the System i. These values determine the maximum number of sign-on attempts per user, which users can sign-on, how they can sign-on, and when and where sign-on can be performed.

Importance	Description	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
	**Displays sign-on information.** This system value controls whether the user sees an informational display at sign-on that contains the date and time of the most recent sign-on and the number of invalid sign-on attempts since then.	QDSPSGNINF	0	1	By knowing the last time this user signed-on, the user or the system administrator can verify that no one else is using this user's profile.	 0
	**Limit device session** Controls whether a user can sign-on at more than one work station. This does not prevent the user from using group jobs or making a system request (pressing the System Request key) at the same work station.	QLMTDEVSSN	0	1	Prevents someone else from using a user profile at the same time as someone else.	 0
	**Limit security officer device access.** Controls whether users with *ALLOBJ or *SERVICE special authority need explicit authority in order to access specific work stations.	QLMTSECOFR	0	1	Prevents the risk that users with powerful user profiles will sign-on from a remote terminal.	 0
	**Maximum sign-on attempts allowed** Incorrect sign-on attempts on secured systems (security level 20 or higher, see the system value QSECURITY) can occur as a result of any of the following circumstances: o Incorrect User ID o Incorrect Password o The user profile does not have authority to access the device from which the user ID was entered	QMAXSIGN	9	3	The higher this value, the more often the user can attempt to access the system.	 0
	**Maximum sign-on attempts action** Specifies how the system reacts when the maximum number of consecutive, incorrect, sign-on attempts (the system value QMAXSIGN) is reached. A change to this system value takes effect the next time someone attempts to sign on.	QMAXSGNACN	2	3	Improper setting of this parameter may enable hackers and/or hacking software to re-attempt breaking this password.	 50
	**Remote sign on** Specifies how the system handles remote sign-on requests.	QRMTSIGN	iSecurity	*FRCSIGNON	Sign-on requests from remote terminals require special attention in order to ensure that only authorized users enter the system.	 100
	**Retain server security** Determines whether the security data needed by a server to authenticate a user on a target system through client-server interfaces can be retained on the host system	QRETSVRSEC	1	0	Retaining security information is never recommended.	 0

Score with iSecurity: 
Score: 
Explanation: The computer's settings are invalid and pose immediate security threats. **iSecurity User Sign On functionality should be implemented.**

Top

* * * * *

3.2 Use of Adopted Authority

Adopted authority can be considered a "master key" into the system, which is why this subject has special importance. The System Administrator should check the inventory of programs which adopt authority and which programs were added- iSecurity provides such reports.

Importance	Description	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
	**Use adopted authority** Defines which users can create programs with the Use Adopted Authority (*USEADPAUT(*YES)) attribute. All users can create, change, or update programs and service programs to use adopted authority if the user has the necessary authority to access the program or service program.	QUSEADPAUT	ADPAUT	Authorization list	Use adopted authority	 100

Score with iSecurity: 
Score: 
Explanation: The computer's Adopted Authority security is perfect; the System Administrator can control who creates such programs but cannot review program usage.

Top

* * * * *

3.3 Unattended terminals

Importance	Description	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
	**Inactive job time out** Specifies when the system takes action on inactive interactive jobs. The system value QINACTMSGQ determines the action the system takes. Local jobs that are currently signed-on to a remote system are excluded.	QINACTITV	*NONE	15	Unattended terminals are very large risks; they enable anyone to easily use existing programs to access and modify data. iSecurity's Screen module controls screen activity time based on location/user.	 0
Information Only	**Inactive message queue** Inactive message queue	QINACTMSGQ	*ENDJOB	*DSCJOB	It is recommended not to leave jobs in inactive status.	Information Only
Information Only	**Disconnect job interval** Specifies the length of time in minutes an interactive job can be disconnected before it is ended. An interactive job can be disconnected with the DSCJOB command or when an I/O error occurs at the interactive job's work station (the system value QDEVRCYACN).	QDSCJOBITV	5	240	An interactive job must not be left idle for any length of time.	Information Only

Score with iSecurity: 
Score: 
Explanation: Computer settings are faulty. **Avoid a possible security threat to the network by implementing iSecurity Screen.**

Top

* * * * *

3.4 Miscellaneous Sign-on

Importance	Description	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
50	**Remote power on and IPL** Specifies whether remote power on and IPL can be started over a telephone line.	QRMTIPL	0	0	The ability to turn on the computer from a remote site may enable IPL at times when it is not possible to secure the computer, i.e. public holidays, or at times before new security policies are applied.	★★★★★ 100
50	**Allow object restore** Specifies whether or not objects with security-sensitive attributes can be restored. This value is made up of a list of values that control the object being restored.	QALWOBJRST	*ALL	*ALWPTF	Restoring of unidentified and unauthorized products may enable entry of viruses and Trojan horses.	☆☆☆☆☆ 0
50	**Remote service attribute** This system value controls the remote system service problem analysis ability. The value allows the system to be analyzed remotely.	QRMTSRVATR	0	0	Anyone entering the computer is a potential risk. This value enables remote companies to analyze problems and service the computer.	★★★★★ 100

Score with iSecurity: ★★★★★
Score: ★★★☆☆
Explanation: Some miscellaneous sign-on values are in accordance with industry standards. However, the computer's scores are borderline and should be reviewed.

Top

* * * * *

3.5 Password Control

Password values provide the initial level of protection in any effective security policy.

Importance	Password system value	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
100	**Days password is valid** Password expiration interval. Specifies the number of days for which passwords are valid. This provides password security by requiring users to change their passwords after a specified number of days. If the password is not changed within the specified number of days, the user cannot sign-on until the password is changed. Seven days before the password ends, the user is warned at sign-on.	QPWDEXPITV	*NOMAX	60	To avoid any possible intrusions, passwords must be changed frequently.	0
100	**Minimum password length** Specifies the minimum number of characters in a password.	QPWDMINLEN	5	6	An effective password must be long enough to baffle intruders/hackers, but short enough to be easily remembered without being written down.	50
50	Maximum password length Specifies the maximum number of characters in a password.	QPWDMAXLEN	10	8	This provides additional security by preventing users from specifying passwords that are too long and need to be recorded somewhere because they cannot be easily remembered.	100
100	**Duplicate password control** This system value limits how often a user can repeat the use of a password.	QPWDRQDDIF	0	7	An effective security policy mandates that passwords must be changed frequently to maintain confidentiality.	0
50	**Limit characters in a password** This provides password security by preventing certain characters (vowels, for example) from appearing in a password, making it difficult to guess passwords by preventing the use of common words or names as passwords.	QPWDLMTCHR	*NONE	AEIOU@#$	Easy-to-guess passwords provide an open invitation to intruders and hackers.	0
50	**Limit adjacent digits in a password** Specifies whether adjacent numbers are allowed in passwords. This makes it difficult to guess passwords by preventing the use of dates or social security numbers as passwords.	QPWDLMTAJC	1	1	To avoid hackers and possible intruders, it is necessary to formulate passwords that are difficult to guess.	100
50	**Limit repeating characters** Limit repeating characters in password. This prevents a user from using the same character more than once in the same password. (For example, AAAA)	QPWDLMTREP	0	2	Repetitive characters increase the chances of that password being stolen.	0
50	**Limit character's positions** Positions the list. Specify *TOP, *BOT, or the starting characters of the system value which is being searched for.	QPWDPOSDIF	0	1	Position the search with the password entered.	0
50	**Required digits in password** Specifies whether a specific digit is required in a new password.	QPWDRQDDGT	0	1	Because this value prevents the user from only using alphabetic characters, the chances of the password being guessed by an intruder are decreased.	0
	Password validation program				Additional	

100	This provides the ability for a user-written program to do additional validation on passwords.	QPWDVLDPGM	*REGFAC	iSecurity	validation results in increased password security.	★★★★★ 100
100	Password level	QPWDLVL	0	3	Password level	☆☆☆☆☆ 0

Score with iSecurity: ★★★★★
Score: ★☆☆☆☆
Explanation: Computer settings are faulty and open to password-related security threats. **iSecurity Password should be implemented.**

Top

* * * * *

3.6 Activation of Network Protection

Exit points of the operating system Registration Facility are checked only if the value of PCSACC is *REGFAC. If a program name exists instead, security controls may still be present, although with serious performance degradation.

Importance	Parameter Name	Value	Recommended Value	Risk
100	PCSACC	*REGFAC	*REGFAC	If a program name is specified, this is the name of the customer supplied Client Access/400 host system application exit program that can supplement system object level authority, restricting requests from the client. *REGFAC specifies that the system will use the registration facility to determine which exit program if any is to run. If no exit program is defined for an exit point, and *REGFAC is specified, then *OBJAUT is used instead. *OBJAUT specifies that normal object authorizations are checked for this client request and is not recommended.

Score: ★★★★☆

Explanation: Most of the computer's exit points are protected; minor revisions will enable the computer to be fully protected. **iSecurity Firewall is the only product on the market which controls and manages all security-related IBM i exit points and is required in a PC-emulated environment.**

3.6.1 Registration Facility Exit Points Protection

Exit Points, if unprotected, provide unauthorized access to the System i. It is vital that security policies protect all Exit Points. Note that in some cases standard IBM programs may appear (starting with the letter Q). Such programs are not considered security programs.

Importance	Exit point	Program name	Current Score
100	Original File Transfer Function	iSecurity	★★★★★ 100
100	FTP Server Logon (format: TCPL0100)		☆☆☆☆☆ 0
100	FTP Server Logon (format: TCPL0200)		☆☆☆☆☆ 0
100	FTP Server Logon (format: TCPL0300)		☆☆☆☆☆ 0
100	FTP Server-Incoming Rqst Validation		☆☆☆☆☆ 0
100	FTP Client-Outgoing Rqst Validation		☆☆☆☆☆ 0
100	TFTP Server Request Validation	iSecurity	★★★★★ 100
100	REXEC Server Logon		☆☆☆☆☆ 0
100	REXEC Server Request Validation	iSecurity	★★★★★ 100
100	Original Remote SQL Server	iSecurity	★★★★★ 100
100	Database Server - SQL access & Showcase	iSecurity	★★★★★ 100
100	Database server -SQL access	iSecurity	★★★★★ 100
100	Databse showcase	GSCCASQ@R	★★★★★ 100
100	Database Server - data base access (format: ZDAD0100)	iSecurity	★★★★★ 100
100	Database Server - data base access (format: ZDAD0200)	iSecurity	★★★★★ 100
100	Remote Command/Program Call	iSecurity	★★★★★ 100
100	File Server	iSecurity	★★★★★ 100
100	Telnet Device Initialization	iSecurity	★★★★★ 100
100	Telnet Device Termination	iSecurity	★★★★★ 100
100	Sign-On Completed	iSecurity	★★★★★ 100
100	Original Data Queue Server	iSecurity	★★★★★ 100
100	Data Queue Server	iSecurity	★★★★★ 100
100	Original Virtual Print Server	iSecurity	★★★★★ 100
100	Original License Mgmt Server	iSecurity	★★★★★ 100
100	Central Server - license mgmt	iSecurity	★★★★★ 100
100	Central Server - conversion map	iSecurity	★★★★★ 100

100	Central Server - client mgmt	iSecurity	100
100	Network Print Server - entry	iSecurity	100
100	Network Print Server - spool file	iSecurity	100
100	Original Message Server	iSecurity	100
100	Database Server - entry	iSecurity	100
100	Database Server - object information (format: ZDAR0100)	iSecurity	100
100	Database Server - object information (format: ZDAR0200)	iSecurity	100
100	Change User Profile	iSecurity	100
100	Create User Profile	iSecurity	100
100	Delete User Profile - after delete	iSecurity	100
100	Delete User Profile - before delete	iSecurity	100
100	Restore User Profile	iSecurity	100
100	TCP Signon Server	iSecurity	100
100	Prepower Down System	iSecurity	100
100	DHCP Address Binding Notify	iSecurity	100
100	DHCP Address Release Notify	iSecurity	100
100	DHCP Request Packet Validation	iSecurity	100

3.6.2 Anti Virus

Importance	Exit point	Program name	Current Score
100	Integrated File System Scan on Open Exit Program		0
100	Integrated File System Scan on Close Exit Program		0

Top

* * * * *

3.7 Auditing System and User Activities

System auditing provides tools to assess and review computer security policies for efficiency and consistency of implementation.
Note: If the value "*AUDLVL" is set to "Off", all values except for "*OBJAUD" are irrelevant.

Importance	Value	Description	Set	Current Score
100	*AUDLVL	**System Audit** Auditing changes controlled by the QAUDLVL system value and CHGUSRAUD command or AUDLVL keyword are implemented.	On	100
100	*OBJAUD	**Object Audit** Performs auditing of objects that have been selected for audit using the CHGOBJAUD command.	On	100
100	*AUTFAIL	**Authorization Failure** The following authorization failures are audited: o All access failures (sign-on, authorization, job submission) o Incorrect password or user ID entered from a device	On	100
50	*CREATE	**Object Creation** o Objects created into library QTEMP are not audited. The following objects are audited: o Newly-created objects o Objects created to replace an existing object	On	100
100	*DELETE	**Object Deletion** All deletions of external objects on the system are audited. Objects deleted from library QTEMP are not audited.	On	100
100	*JOBDTA	**Job task** Audits certain actions by audited users.	On	100
100	*NETCMN	**Communication and Network task** All violations detected by the APPN firewall function are audited. The two journal entry types are: o NE - Auditing of End point filter violations o ND - Auditing of Directory search filter violations	On	100
100	*OBJMGT	**Object management** The following generic object tasks are audited: o Moving objects o Renaming objects	On	100
50	*OFCSRV	**Office task** The following OfficeVision/400 tasks are audited: o Changes to the system distribution directory o Tasks involving electronic mail	On	100
50	*OPTICAL	**Optical task** The following optical functions are audited: o Add or remove optical cartridge o Change the authorization list used to secure an optical volume o Open optical file or directory o Create or delete optical directory o Change or retrieve optical directory attributes o Copy, move, or rename optical file o Copy optical directory	On	100
100	*PGMADP	**Adopted Authority program** Adopting authority from a program owner is audited.	On	100
100	*PGMFAIL	**Infringement of System integrity** The following program failures are audited: o Blocked instruction o Validation value failure o Domain violation	On	100
100	*PRTDTA	**Printing functions** The following printing functions are audited: o Printing a spooled file o Printing with parameter SPOOL(*NO)	On	100
100	*SAVRST	**Object restore** The following save and restore information is audited: o When programs that adopt their owner's user profile are restored o When job descriptions that contain user names are restored o When ownership and authority information change for restored objects o When the authority for user profiles is restored o When a system state program is restored o When a system command is restored	Off	0
100	*SECURITY	**Security task** All security-related functions are audited, including: o Changes to object authority o Create, change, delete, and restore user profiles operations o Changes to object ownership	Off	0

		o Changes to programs (CHGPGM) that will now adopt the owner's profile o Changes to system values and network attributes o Changes to subsystem routing o When the QSECOFR password is reset to the shipped value by DST o When the DST security officer password is requested to be defaulted		
	*SERVICE	**HW/SW Service** The following commands are audited: o Dump Object (DMPOBJ) and Dump System Object (DMPSYSOBJ) o Start System Service Tools (STRSST): one entry is sent when the STRSST is used to enter the service tools. o Start Service Job (STRSRVJOB): the trace commands do not produce an audit record. o Start Copy Screen (STRCPYSCN) o Start, End, Print, and Delete Communications Trace o Trace Internal (TRCINT) o Print Error Log (PRTERRLOG) o Print Internal Data (PRTINTDTA)	Off	 0
	*SPLFDTA	**Spool Management** The following spooled file functions are audited: o Create a spooled file o Delete a spooled file o Display a spooled file o Copy a spooled file o Get data from a spooled file (QSPGETSP) o Hold a spooled file o Release a spooled file o Change spooled file attributes (CHGSPLFA command)	Off	 0
	*SYSMGT	**System Control** The following system management tasks by an audited user are audited: o Hierarchical file system registration o Changes for Operational Assistant functions o Changes to the system reply list o Changes to the DRDA relational database directory o Network file operations	Off	 0
	*NETBAS	**Network base functions are audited.** The following are some examples: o IP rules actions o Sockets connections o APPN Directory search filter o APPN end point filter	Off, but in effect (*NETCMN On)	 100
	*NETCLU	**Cluster or cluster resource group operations are audited.** The following are some examples: o Add, create, and delete o Distribution o End o Fail over o List information o Removal o Start o Switch o Update attributes	Off, but in effect (*NETCMN On)	 100
	*NETFAIL	**Network failures are audited.** The following are some examples: o Socket port not available	Off, but in effect (*NETCMN On)	 100
	*NETSCK	**Sockets tasks are audited.** The following are some examples: o Accept o Connect o DHCP address assigned o DHCP address not assigned o Filtered mail o Reject mail	Off, but in effect (*NETCMN On)	 100
	*SECCFG	**Security configuration is audited.** The following are some examples: o Create, change, delete, and restore operations of user profiles o Changes to programs (CHGPGM) that will now adopt the owner's profile o Changes to system values, environment variables and network attributes o Changes to subsystem routing o When the QSECOFR password is reset to the shipped value from DST o When the password for the service tools security officer user ID is requested to be defaulted. o Changes to the auditing attribute of an object.	Off	 0
		Changes or updates when doing directory service functions are audited. The following are some examples:		

	*SECDIRSRV	o Audit change o Successful bind o Authority change o Password change o Ownership change o Successful unbind	Off	0
	*SECIPC	**Changes to interprocess communications are audited** The following are some examples: o Ownership or authority of an IPC object changed o Create, delete or get of an IPC object o Shared memory attach	Off	0
	*SECNAS	**Network authentication service actions are audited** The following are some examples: o Service ticket valid o Service principals do not match o Client principals do not match o Ticket IP address mismatch o Decryption of the ticket failed o Decryption of the authenticator failed o Realm is not within client and local realms o Ticket is a replay attempt o Ticket not yet valid o Ticket is a replay attempt o Remote or local IP address mismatch o Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error o RKRB_AP_PRIV or KRB_AP_SAFE - timestamp error, replay error, sequence order error o GSS accept - expired credentials, checksum error, channel bindings o GSS unwrap or GSS verify - expired context, decrypt/decode, checksum error, sequence error	Off	0
	*SECRUN	**Security run time functions are audited** The following are some examples: o Changes to object ownership o Changes to authorization list or object authority o Changes to the primary group of an object	Off	0
	*SECSCKD	**Socket descriptors are audited** The following are some examples: o A socket descriptor was given to another job o Receive descriptor o Unable to use descriptor	Off	0
	*SECVFY	**Use of verification functions are audited** The following are some examples: o A target user profile was changed during a pass-through session o A profile handle was generated o All profile tokens were invalidated o Maximum number of profile tokens has been generated o A profile token has been generated o All profile tokens for a user have been removed o User profile authenticated o An office user started or ended work on behalf of another user	Off	0
	*SECVLDL	**Changes to validation list objects are audited** The following are some examples: o Add, change, remove of a validation list entry o Find of a validation list entry o Successful and unsuccessful verify of a validation list entry	Off	0

Score with iSecurity:
Score:
Explanation: Most of the computer's auditing policies are not in place and therefore pose a possible security threat. **iSecurity Audit should be implemented.**

Top

* * * * *

3.8 Users Class

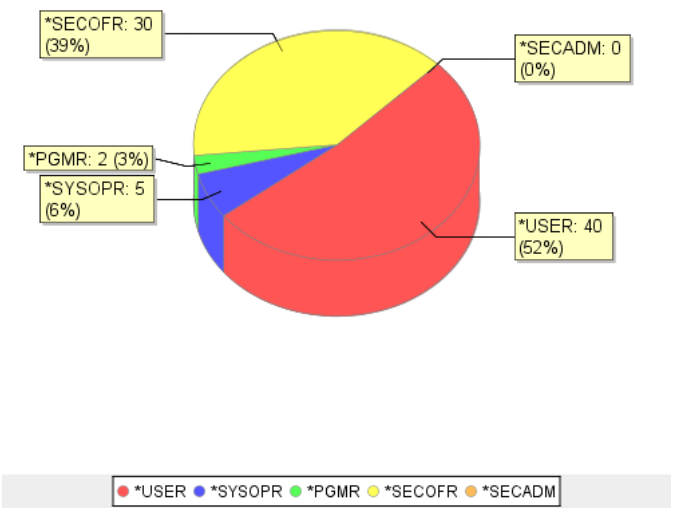
"Users Class" is checked only when the user profile has the attribute of "*USRCLS" in its Special Authorities parameter.An effective security policy mandates that the number of users with *SECOFR and *SECADM authority must be limited in order to control access to classified data. Users with Special Authorities were granted this authority based upon their User Class.

Total number of users: 0.

Importance	User Class	Description	Number of Enabled Users	Number of Disabled Users	Recommended Value	Current Score
Information Only	*USER	User	40	120		Information Only
Information Only	*PGMR	Programmer	2	31		Information Only
Information Only	*SYSOPR	System operator	5	16		Information Only
	*SECADM	Security administrator	0	1	0-3	 100
	*SECOFR	Security officer	30	62	0-3	 0

Score with iSecurity: 
Score: 
Explanation: This number is too high for proper security; review security policies and reduce the number of power users. **iSecurity Audit should be implemented.**

Distribution Of Users



Top

* * * * *

3.9 Analyzing Users By Privilege

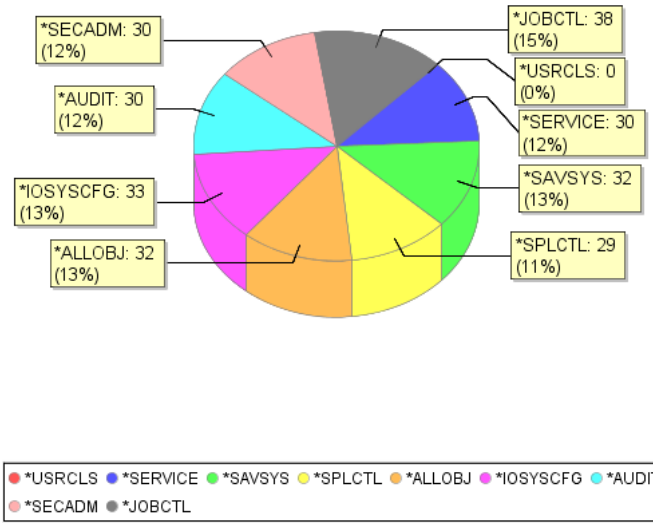
Proper security policies mandate caution in designating security privileges. Therefore, *ALLOBJ and other special authorities should be restricted to a minimal number of users.

Total number of users: 0.

Importance	User Privilege	Description	Number of Enabled Users	Number of Disabled Users	Recommended Value	Current Score
100	*ALLOBJ	All object authority is granted for accessing any system resource	32	94	0-3	0
100	*AUDIT	Allows the user to perform auditing functions	30	65	0-3	0
100	*IOSYSCFG	Allows changes to system configuration	33	70	0-3	0
100	*JOBCTL	Allows manipulation of job and output	38	104	0-5	0
100	*SAVSYS	Used for saving and restoring the system and data without having explicit authority to objects, queues, and subsystems	32	71	0-3	0
100	*SECADM	Allows administration of user profiles	30	70	0-3	0
100	*SERVICE	Allows access to special service functions for problem diagnosis	30	68	0-3	0
100	*SPLCTL	Allows control of spool functions	29	72	0-5	0
50	*USRCLS	Special authorities are granted based on User Class	0	0	0-3	Information Only

Score with iSecurity: ★★★★★
Score: ☆☆☆☆☆
Explanation: Since you have greatly exceeded the number of recommended privileged users, enterprise data is far too easily accessible. The System Administrator should reduce that number immediately. **iSecurity Audit should be implemented to manage and possibly disable all network access, and especially activities generated from users having All Object Authority.**

Distribution Of Users



Top

* * * * *

3.10 Users with default password

Default passwords are easy-to-guess for potential intruders, and therefore pose a high security risk. This risk becomes real and immediate if the users are enabled; otherwise the risk remains dormant.

Total number of users: 0.

Importance	Description	Number	Recommended Value	Current Score
50	Number of users with default password	109	0	0
100	Enabled users with default password (Very High Risk)	8	0	0

Score with iSecurity:
Score:
Explanation: The number of enabled users with a default password is much too high and poses a serious security risk. **Reduce the number of enabled users and implement iSecurity Password.**

Top

* * * * *

3.11 Users with command line access

Command line authority for an IBM i user can be very dangerous. A user with Command Line Authority can use commands such as ENDJOB, DLTJOB, etc., which can be very harmful.

Total number of users: 0.

Importance	User Capabilities	Description	Number	Recommended Value	Current Score
100	*NO *PARTIAL	Number of users, that are defined in "*USER" class and that have "*Enabled" status, having full command line access or partial command line access.	38	0	0

Score with iSecurity:
Score:
Explanation: : This number is too high and poses a security risk. **Reduce the number of users with command line access.**

Top

* * * * *

3.12 Network Access via Port

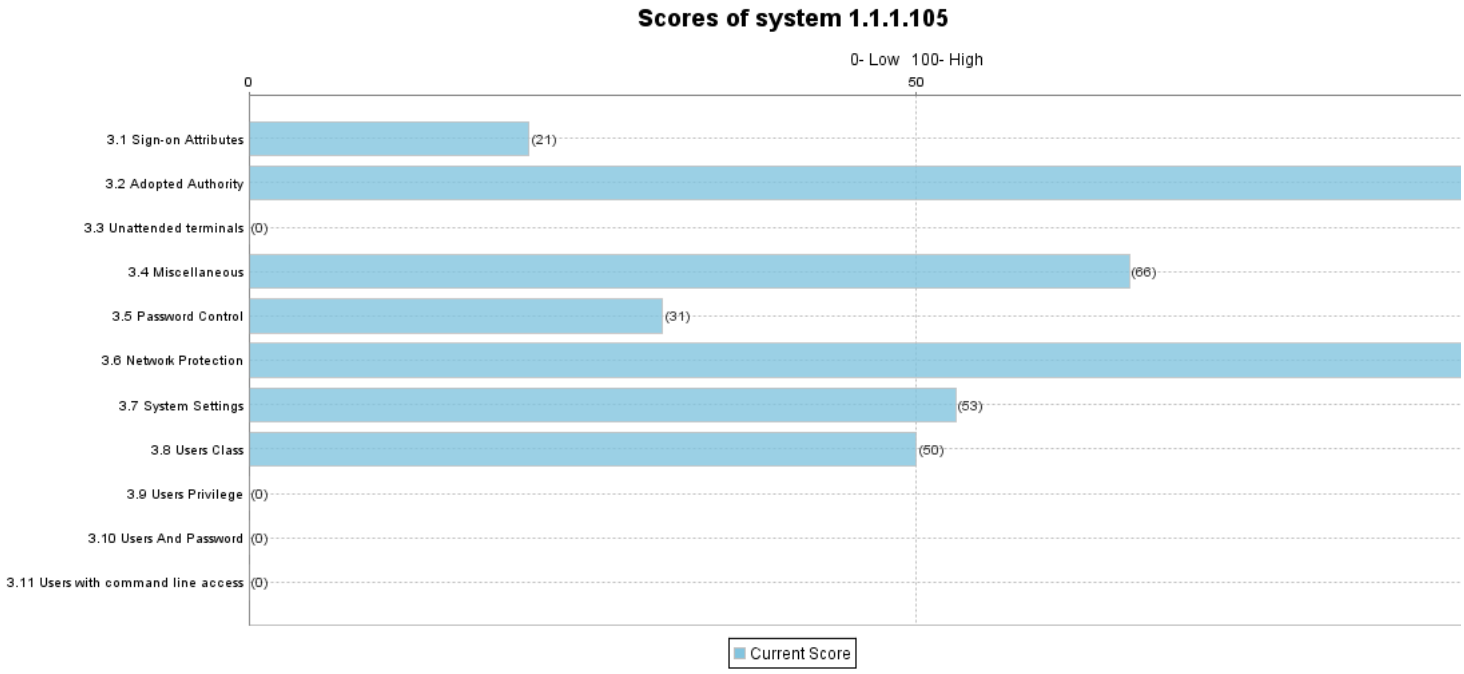
The default authorization for TCP/IP ports is allow any user profile access to any port. The current open ports in the system are the following.

Port Name	Port Number
as-file	8473
as-netprt	8474
as-rmtcmd	8475
as-dtaq	8472
as-database	8471
as-central	8470
as-signon	8476

Top

* * * * *

3.13 Scores of system 1.1.1.105



Top

* * * * *

Final Score :

Explanation: Total computer scores reveal several flaws in the system. The System Administrator should immediately revise the computer's security policies or risk facing a possible security threat.

Top

* * * * *

4. Contact Information

Raz-Lee Security
Tel (U.S): 1-888-7295334
Tel (Worldwide): +972-9-9588860
www.razlee.com
assessment@razlee.com

Top

* * * * *

Generated by Assessment 2.2.0