GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

AS/400? An Auditing How-To
Layton Welborn
April 10, 2001

Introduction

This is article is for those of us out there who not only have *nix and Windows machines on their networks but also another type of machine, namely the AS/400. [Note: just recently, IBM has re-branded the AS/400 as the new **iSeries** server] When exploring the numerous computer security sites on the Internet, a plethora of information is available to audit and secure Windows[+] and *nix machines. As for the AS/400, information is limited to just a few sites and for the most part, the AS/400 has been kept "in the closet". This article will summarize how to implement and use the AS/400 to develop a "Poor Man's Auditing System" utilizing the tools that are delivered with the operating system.

Security Functions Standards

IBM has the following categories available in the operating system for auditing. These six security categories should be implemented in a company's security policy. These are the various items that make up complete security and also adhere to the confidentiality, integrity, and availability rule for protection.

- **Identification and authentication:** Identifies users to the system and provides proof that they are who they claim to be.
- **Access control:** Determines which users can access which resources.
- **Data confidentiality:** Protects an organization's sensitive data from unauthorized disclosure.
- **Data integrity:** Ensures that data is in its original form and that it has not been altered.
- **Security management:** Administers, controls and reviews a business' security policy.
- **Nonrepudiation:** Assures that the message was sent by the appropriate individual.[1]

These are in accordance with the ISO 7498-2 standard.

Set up Auditing

Auditing is not activated by default when an AS/400 is shipped; therefore it needs to be activated. This can be done by issuing the following steps: (*Commands are printed inside [ ])*

1. Create a library to hold the auditing data (a journal receiver). In this example *auditlib* will be used. [CRTLIB LIB(auditlib) TEXT('My Auditing Library')]
2. Set the library's authority to *EXCLUDE for *PUBLIC use. This will prevent other users from being allowed to view the library. [GRTOBJAUT OBJ(*LIBL/auditlib) OBJTYPE(*LIB) USER(*PUBLIC) AUT(*EXCLUDE) REPLACE(*YES)]
3. Set Auditing Levels and Start Auditing [CHGSECAUD QAUDCTL(*AUDLVL OBJAUD NOQTEMP) QAUDLVL(*AUTFAIL *SECURITY *DELETE *OBJMGT) JRNRCV(*auditlib*/AUDRCV0001]

   QAUDLVL determines the level of auditing you want the system to perform. There are 16 possible settings, and you can specify any number of them except where they exclude each other:

   - *NONE means system-wide auditing isn't done, but auditing is performed for users who have a value other than *NONE specified in the AUDLVL parameter of their user profiles.
   - *AUTFAIL means unsuccessful log-on attempts and unauthorized attempts to use sensitive objects are audited. These include rejected connection attempts, invalid network sign-on attempts, and attempts to perform an operation or access an object to which

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the user isn't authorized.

- *CREATE means the creation of new objects or objects that replace existing objects is audited.
- *DELETE means the deletion of objects is audited.
- *JOBDTA means start, change, hold, release, and end job operations are audited. This includes server sessions and remote connection jobs.
- *NETCMN means violations detected by the APPN Filter support are audited.
- *OBJMGT means object rename and move operations are audited.
- *OFCSRV means OfficeVision for OS/400 tasks (e.g., changing the system distribution directory, opening a mail log) are audited.
- *PGMADP means gaining access to objects via program adopted authority is audited.
- *PGMFAIL means programs that run a restricted machine interface instruction or access objects via an unsupported interface are audited.
- *PRTDTA means printing job output is audited whether the output is sent directly to a printer, sent to a remote system, or spooled and printed on a local machine.
- *SAVRST means save and restore operations are audited.
- *SECURITY means a wide range of security-related activities are audited, including:
    - changing an object's audit value or a user's audit setting
    - changing an authorization list or an object's authority
    - changing an object's ownership
    - creating, restoring, or changing a user profile
    - requests to reset the DST QSECOFR password
    - generating a profile handle through the QSYGETPH API
    - changing a network attribute, system value, or service attribute
- ***SERVICE means starting, pausing, and stopping servers and using service tools are audited.
- *SPLFDTA means creating, changing, holding, and releasing spooled files is audited. An audit journal entry will also be written when someone other than the owner of a spooled file views it.
- *SYSMGT means changing backup options, automatic cleanup options, and power on/off schedules using Operational Assistant is audited. Changing the system reply list and access path recovery times is also audited.[2]

Once these three steps are completed auditing is started on the AS/400.

Now What?

Now that Auditing has been started, you can start running daily, weekly, and/or monthly reports of the data that is collected in the auditing journal. Fortunately, as part of the standard installation, IBM includes the SECTOOLS menu.(Figure 1) [just type **GO SECTOOLS** on a command line]. Using this menu, you can run individual reports or submit all the reports to run in batch mode. The important report is option 22 – Audit journal entries. This is the report that will allow you to view the different types of auditing entries that are recorded in the audit journal. (see Table 1) Multiple types can be specified to construct an informative report suitable for auditing. The AS/400 allows the ability to schedule these reports to run automatically using the AS/400 Job Scheduler. [e.g. **ADDJOBSCDE JOB(COREPORT) CMD(DSPJRN JRN(QAUDJRN) ENTTYP(*co*) FRQ(*MONTHLY) SCDTIME('02:00')**]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table 1 – **Journal Entry Types**

AF Authorization failure entries.	**PG** Change of an object's primary group.
CA Change authority entries.	**PO** Printed output entries.
CD Command string entries.	**PW** Invalid password entries.
CO Create object entries.	**SF** Action on spooled files entries.
CP Change user profile entries.	**SV** System values changed entries
DO Delete object entries.	**VO** Validation list actions
JS Actions against jobs entries.	**YR** DLO object read entries
ND Directory search filter violations.	**YC** DLO object changed entries
NE End point filter violations.	**ZR** Object read entries
OR Object restored entries.	**ZC** Object changed entries
OW Object ownership changed entries	

Day-to-Day Auditing Tasks

Even though a system has been configured and secured, it is difficult to maintain that same level of security if you have users signing onto the box daily. Due to this factor, some sort of daily monitoring has to be incorporated into the operation of the AS/400 because "security…tends to deteriorate over time."[1] The typical factors are:

- New objects created by system users
- New users enrolled on the system
- Changes of object ownership – authorization not adjusted
- Changes of responsibilities – user group changed
- Temporary authorizations – not revoked
- New products installed
- Maintenance applied – security level lowered and not reset, and so on[1]

1. **Status Monitoring** – Monitoring of key security controls should include.
   a. Global Controls and Options at the System Level (e.g. Physical Security and maintaining/verifying changes to System Values) [DSPJRN JRN(QAUDJRN) ENTTYP(SV)]
   b. Critical User Profiles – Profiles with special authorities and IBM-supplied profiles need to be checked and verified that the profile:
      1. Does not have a default password. [DSPAUTUSR OUTPUT(*PRINT)]
      2. Does not have authority to objects, devices, commands, etc. it does not explicitly need. [DSPUSRPRF USRPRF(*userprofile*) TYPE(*ALL) OUTPUT(*PRINT)]
      3. Verify that default users have a password of *NONE and that they are not allowed to signon to the system. [*same command as above*]
   c. Critical Objects – Public and specific authority should be checked to meet the current security policy.
2. **Event Monitoring** – Monitoring of key security events should be done in the following

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

priority.

a. Analyze the changes to security definitions and rules.
b. Analyze access to critical objects: [DSPOBJAUT OBJ(library/object) OBJTYPE(type) OUTPUT(*PRINT)]
c. Analyze attempted violations: The following command would print authorization failures.[DSPJRN JRN(QAUDJRN) ENTTYP(AF) OUTPUT(*PRINT)]

Periodic Reviews (Monthly/Semi-Annual/Annual)

Periodic Reviews can consist of highly detailed scrutiny of the AS/400 system or just a more "diagnostic" review of objects. Currently, my company's policy involves monthly review of all security related items on our AS/400s. These include the following:

1. **Security-Related System Values** – [WRKSYSVAL SYSVAL(*SEC) OUTPUT(*PRINT)] This report is reviewed to verify that the values are at the required level.
2. **User and Group Definitions** – [DSPUSRPRF USRPRF(*ALL) TYPE(*ALL) SELECT(*SPCAUT) SPCAUT(*ALL)] This is to identify the power users/security officers and verify that no other profile has received unauthorized authorities.
3. **Access Authorization** – This report is given to list all the objects in a given library and displays their owners and authorities on the object. [DSPOBJAUT OBJ(object_name) LIB(library_name) OBJTYPE(*ALL) OUTPUT(*PRINT)]

Conclusion

The AS/400 has integrated security throughout its design and implementation and therefore has the ability to keep track of an enormous amount of information. Once configured, one can keep detailed records of security information and be able to audit their AS/400 with relative ease. There are plenty of excellent third-party tools available that you can purchase that automate this process, but the OS/400 is packed with easy to use tools that can help this cause along. Auditing the AS/400 does not have to be something that you spend thousands of dollars to do, but can be done using the tools that are already present.

References

1. IBM Corporation. "An Implementation Guide for AS/400 Security and Auditing: Chapter 14, Auditing the AS/400." 01 Jun 1994.
URL: http://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg244200.pdf

2. Azubike Oguine. "Using AS/400 Security Auditing." Jun 2000.
URL: http://www.as400network.com/resources/artarchive/index.cfm?fuseaction=viewarticle&CO_ContentID=7454&OCFI=2980741&OCFT=76220851

Carol Woodbury. "Taking a Stand with AS/400 Security." Jan 1999.
URL:
http://www.as400network.com/artarchive/index.cfm?fuseaction=viewarticle&ArticleID=13182

Denis Seiler. "Keep an Eye on Your AS/400 with Auditing." Feb 1999.
URL: http://www.as400network.com/resources/artarchive/index.cfm?fuseaction=viewarticle&CO_ContentID=2594

IBM Corporation. "Tips and Tools for Securing Your AS/400: Chapter 4, Security Tools." 26 Jun 1998.
URL: http://publib.boulder.ibm.com/cgi-bin/bookmgr/BOOKS/qb3acf02/CCONTENTS

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.