

Hacking AS400 / iSeries



By Shalom Carmel

Trademarks

The following are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Advanced Function Printing	ibm.com®
Advanced Peer-to-Peer Networking®	ILS/400®
AFP	iNotes
AFS®	Intelligent Printer Data Stream
AIX®	IP PrintWay
alphaWorks®	IPDS
AnyNet®	iSeries
Application System/400®	Lotus Notes®
AS/400®	Lotus®
AS/400e	MQSeries®
BookManager®	Net.Commerce
C/400®	Net.Data®
CICS/400®	NetRexx
COBOL/400®	Notes®
DB2 Client Application Enablers	OfficeVision/400
DB2 Connect	Operating System/400®
DB2 Extenders	OS/400®
DB2 OLAP Server	Power Series 400®
DB2 Universal Database	QMF
DB2®	Redbooks
developerWorks®	RPG/400®
Domino Designer®	SAA®
Domino.Doc®	SQL/400®
Domino®	System/36
DPI®	System/38
DRDA®	Systems Application Architecture®
Electronic Service Agent	WebSphere®
IBM Electronic Services for AS/400®	

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of the companies mentioned above or of others.

Disclaimer of Warranty

The author makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages. While every precaution has been taken in the preparation of this publication, the author assumes no responsibility for errors or omissions. This publication and features described in it are subject to change without notice. The information contained herein is provided for educational purposes only.

Copyright Notice

© 2004, 2005, by Shalom Carmel. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Shalom Carmel, except for making a personal backup copy, and except for printing a copy for personal use.

Book contents at a glance

<i>Introduction</i>	<i>1</i>
<i>Chapter 1: Server footprinting</i>	<i>3</i>
<i>Chapter 2: User Enumeration</i>	<i>11</i>
<i>Chapter 3: Getting unplanned and unauthorized access</i>	<i>33</i>
<i>Chapter 4: Traps and Trojan horses</i>	<i>79</i>
<i>Chapter 5: Shells and script execution</i>	<i>101</i>
<i>Chapter 6: Hacking the rest of the network through the AS/400</i>	<i>127</i>
<i>Chapter 7: The AS400 on the World Wide Web</i>	<i>147</i>
<i>Chapter 8: Hiding your tracks</i>	<i>159</i>
<i>Chapter 9: Attack exit programs</i>	<i>169</i>
<i>Appendix A: Securing TCP/IP network services</i>	<i>175</i>
<i>Appendix B: Object authority 101</i>	<i>181</i>
<i>Appendix C: Client Access Express</i>	<i>185</i>
<i>Appendix D: References</i>	<i>186</i>
<i>Index</i>	<i>191</i>

Full Table of Contents

Introduction.....	1
Chapter 1: Server footprinting	3
1.1 Port scanning and banner grabbing	3
Telnet.....	5
FTP.....	6
HTTP.....	6
SMTP.....	7
POP3.....	8
SNMP.....	8
Summary	9
Chapter 2: User Enumeration.....	11
2.1 Default users and passwords.....	11
2.2 Network based enumeration.....	12
Sniffing network transport.....	12
Telnet login informational messages	12
POP3 authentication	13
Web server basic authentication	14
Listing iSeries users with FTP	15
LDAP directory services.....	17
Operations Navigator / Client Access.....	20
Brute force password guessing.....	24
2.3 Native mode enumeration.....	26
iSeries users in the Disk Information file.....	26
DSPJOB user profiles disclosure.....	26
Work with User Profiles command	28
Work Object command.....	29
Summary	31
Chapter 3: Getting unplanned and unauthorized access	33
3.1 Gaining command line inside applications	33
Changing the login environment script.....	33
Gaining command line from green screen applications	34
Misconfigured System Request key	35
Accessing system menus from inside applications.....	35
Abusing the ATTN key	36
Application *MENU objects.....	36
Command line at *SIGNOFF.....	36
Application insecure menu options	37
Command Line enabling programs	37
3.2 Escalation of Privileges	38
Switching to another profile.....	38
Modifying user object headers in memory.....	41
Account and authority management	42
3.3 View and modify contents of an AS400 server	45
No terminal necessary.....	45
DB2 to the rescue	52
The traditional way.....	58
Copying back and forth	69
Accessing printed output	70
Integrated File System	74

Summary	77
Chapter 4: Traps and Trojan horses	79
4.1 Meddling with Startup Scripts.....	79
Changing another user's login script.....	79
System IPL startup	81
QSHHELL and PASE startup files.....	82
4.2 Modifying *MENU objects	82
4.3 Hijacking terminal devices.....	84
4.4 Hijacking printed output	85
4.5 Adding payload to events	87
Manipulating command objects	87
Event exit programs.....	91
Message queue trapping.....	92
DB2 trigger programs.....	93
4.6 Hacking work management	93
Scheduled jobs	93
Subsystems	94
4.7 Hacking communications	96
Creating a DRDA Transaction Processing Program.....	96
Changing INETD	97
Adding unplanned TCP/IP services.....	98
Summary	99
Chapter 5: Shells and script execution.....	101
5.1 Scripting/Programming languages	101
CL.....	101
REXX	102
SBMDBJOB, STRDBRDR	103
STRS36PRC	103
Unix clones: QSHHELL and PASE.....	103
C and C++.....	103
Java.....	105
PERL	105
5.2 Remote command execution	105
REXEC server.....	105
Client Access remote command execution	106
DDM – (SBMRMTCMD command)	107
FTP – quote rcmd.....	108
SQL – call any program as stored procedure	108
5.3 Remote interactive access.....	110
HTTP work station gateway.....	110
ASCII TTY Telnet.....	111
Remote QSHHELL server	112
Remote reverse shell using Java RAWT.....	112
Remote reverse shell using netcat	122
X terminal.....	123
VNC Server.....	125
Summary	125
Chapter 6: Hacking the rest of the network through the AS/400.....	127
6.1 Network topology	127
NETSTAT client disclosure.....	127

TRACEROUTE and PING	129
SNMP disclosures	132
Host tables and related files	134
iSeries running BIND	134
NSLOOKUP	135
6.2 TCP/IP clients on the iSeries.....	136
TELNET	136
FTP client	136
Distributed database (DRDA) client.....	136
The Qfilesvr.400 file system	137
Accessing CIFS/SMB resources via QNTC.....	138
NFS client.....	138
6.3 Email abuse	138
6.4 Windows clients.....	140
Attack PC emulations from an iSeries application	140
Virus files on the iSeries.....	144
Summary	144
<i>Chapter 7: The AS400 on the World Wide Web.....</i>	<i>147</i>
7.1 IBM HTTP server	147
JSP source display exposure	147
Denial of service	147
Using validation lists versus system profiles.....	147
Non-hidden directory structure	147
Running scripts as QTMHHTTP1	148
PERL and PHP.....	148
7.2 Net.Data.....	148
Internal variables exposure	148
%define exposure.....	149
Show SQL vulnerability	149
Local path disclosure.....	149
7.3 SQL injection in AS400 context	154
Summary	157
<i>Chapter 8: Hiding your tracks.....</i>	<i>159</i>
8.1 Hiding running jobs from the system admin.....	159
8.2 JOBLOG and printed output.....	159
8.3 QSYSOPR, QSYSMSG message queues	160
8.4 QHST log.....	162
8.5 Audit journal.....	163
8.6 HTTP server logs.....	166
Apache HTTP server	166
Original HTTP server	167
Summary	167
<i>Chapter 9: Attack exit programs</i>	<i>169</i>
9.1 What are security exit programs?	169
9.2 The problem with exit programs	169
Services lacking sufficient exit point validation.....	169
Network attacks.....	169

9.3 Probable exit point validation weaknesses.....	169
FTP directory traversal	170
FTP symbolic link support.....	171
SQL alias and table override.....	171
Cross-schema views, indexes and logical files.....	172
SQL large buffer	172
SQL multiple files join	173
Telnet 5250 extended command support	173
Summary	174
<i>Appendix A: Securing TCP/IP network services.....</i>	<i>175</i>
Securing TCP/IP ports.....	175
Securing services management.....	175
Securing SNMP.....	176
Disabling SNMP	177
Disabling TFTP.....	177
Disabling POP3.....	178
Disabling REXEC	178
Securing Client Access RMTCMD	178
<i>Appendix B: Object authority 101</i>	<i>181</i>
<i>Appendix C: Client Access Express.....</i>	<i>185</i>
<i>Appendix D: References.....</i>	<i>186</i>
Web sites.....	186
Printed and electronic Books	188
iSeries Security applications and vendors	189
<i>Index.....</i>	<i>191</i>

List of Figures

Figure 1: Sample iSeries log in screen	5
Figure 2: Operation Navigator users management.....	21
Figure 3: Operation Navigator user profile details	22
Figure 4: List of authorization lists	23
Figure 5: Authorization list details.....	23
Figure 6: System Request menu.....	26
Figure 7: Display job screen	27
Figure 8: Display job library list	27
Figure 9: List of user profiles from DSPJOB	28
Figure 10: Work with user profiles display	28
Figure 11: Display a user profile display.....	29
Figure 12: Work with authorization lists.....	30
Figure 13: Display authorization list	31
Figure 14: Gaining command line from DSPJOB command	34
Figure 15: Work with Job command	35
Figure 16: Default ATTN menu.....	36
Figure 17: *SIGNOFF display.....	37
Figure 18: QUSCMDLN shell	37
Figure 19: QCMD and QCL shells	38
Figure 20: Work with job descriptions	40
Figure 21: Display a job description	41
Figure 22: Object authority editor.....	44
Figure 23: TFTP configuration	48
Figure 24: View library contents from the IFS side.....	49
Figure 25: View database library contents	50
Figure 26: Select database libraries to work with.....	50
Figure 27: Change table data with Operations Navigator	51
Figure 28: Database change journal warning	51
Figure 29: Create database alias.....	51
Figure 30: Create database alias, continued	52
Figure 31: Native SQL tool (STRSQL).....	53
Figure 32: SQL assistant in Operations Navigator	54
Figure 33: DB2 Query Manager main menu	55
Figure 34: Work with QM queries	55
Figure 35: Work with QM permissions.....	56
Figure 36: Manipulate tables using QM.....	57
Figure 37: Finding a file's journal	57
Figure 38: Work with libraries.....	59
Figure 39: Work with objects command output	60
Figure 40: PDM main screen	61
Figure 41: Work with objects using PDM.....	62
Figure 42: DFU main menu	62
Figure 43: DFU create program - select a file to manipulate	63
Figure 44: DFU create program - turn off audit.....	63
Figure 45: DSPPFM command.....	64
Figure 46: DSPPFM hexadecimal mode	65
Figure 47: Work with links – View list of libraries	68

Figure 48: Work with links – View library contents.....	69
Figure 49: Work with links – view file contents.....	69
Figure 50: Work with spool files	71
Figure 51: Work with printers.....	72
Figure 52: Work with output queue	72
Figure 53: WRKSPLF, basic assistance level	73
Figure 54: Operation Navigator printer output filter.....	73
Figure 55: Operations Navigator – select user for printer output	74
Figure 56: Edit file utility	75
Figure 57: Edit file utility – manage directories	75
Figure 58: Change initial program in a user profile (Operations Navigator)	79
Figure 59: Change initial program in a user profile (native mode).....	80
Figure 60: Display program information.....	80
Figure 61: Display menu attributes	83
Figure 62: Work with message file of menu options	83
Figure 63: Change AS400 menu options.....	84
Figure 64: Display subsystem's sign-on screen	85
Figure 65: Work with LPR output queue	86
Figure 66: Add new printer port in Windows.....	86
Figure 67: Add LPR printer in Windows	87
Figure 68: Display command information.....	88
Figure 69: Display command information, continued.....	89
Figure 70: Work with event exit point registration.....	92
Figure 71: Display subsystem description command output	94
Figure 72: Display routing entry	95
Figure 73: Work with Relational databases.....	96
Figure 74: Work with DDM Files	108
Figure 75: WSG signon screen	110
Figure 76: WSG – AS400 main menu.....	111
Figure 77: Remote AWT daemon.....	112
Figure 78: Remote AWT verification	114
Figure 79: AWT reverse shell sample	115
Figure 80: Another AWT reverse shell sample	116
Figure 81: AWT reverse shell – run AS400 command	118
Figure 82: AWT reverse shell sample – select AS400 command.....	119
Figure 83: AWT reverse shell sample – Prompt AS400 command	120
Figure 84: AWT reverse shell sample – display AS400 command help.....	121
Figure 85: Reverse shell netcat listener.....	122
Figure 86: Launch aixterm.....	124
Figure 87: Launch X terminal.....	124
Figure 88: X terminal display	124
Figure 89: Netstat connection list	128
Figure 90: Netstat connection details	128
Figure 91: Netstat full server name	129
Figure 92: Traceroute job log screen.....	130
Figure 93: Work with DRDA databases.....	137
Figure 94: SMTP relay restrictions	139
Figure 95: SMTP connection restrictions	140
Figure 96: Uninstall REXECD on the PC	143
Figure 97: Net.Data script to run system commands	151

Figure 98: Net.Data script to run any SQL.....	152
Figure 99: Results of Net.Data script to run any SQL	153
Figure 100: Work with QSYSOPR message queue.....	160
Figure 101: OpsNav work with message queues	161
Figure 102: Select message queue to display	161
Figure 103: Work with files command.....	162
Figure 104: Manipulate system auditing	164
Figure 105: Swap audit journal receiver.....	165
Figure 106: Audit Journal Properties	165
Figure 107: Deleting the audit journal receivers.....	166
Figure 108: Remote Command Autostart.....	179
Figure 109: Advanced RMTCMD configuration.....	180
Figure 110: Checking authority flowchart.....	182
Figure 111: Display Object Authority.....	183
Figure 112: CHKOBJ command.....	183

List of Tables

Table 1: Common non-secure ports	4
Table 2: Common secure ports	4
Table 3: Default user profiles	11
Table 4: Telnet, FTP and POP3 comparison for user enumeration	14
Table 5: User profile attributes	43
Table 6: Journal dump file structure	58
Table 7: Comparison between copying commands	70
Table 8: Structure of QATOCSTART file	98
Table 9: Netstat options	127
Table 10: Traceroute options	130
Table 11: Ping options.....	131
Table 12: Summary of object management authorities.....	181
Table 13: Summary of object data authorities	181

Introduction

I started to write this book in the summer of 2001, after reading an audit report done for a client of mine by a leading consulting firm. I was disappointed to see that the only thing they actually looked after were the system values and the user profiles definitions. Although these are two major issues with many AS/400 installations, they are certainly not the only issues. Due to my experience on the platform and to my professional activity in information security, I was already aware of many tricks that compromise security on an AS/400 server. I started to methodically document my bag of tricks, and to actively seek solutions to problems hypothetical hackers intent on abusing an AS400 platform may have.

At that time I was reading my first copy of the successful Hacking Exposed series, and adopted the methodology used there. Some of the more interesting techniques, like running a reverse netcat shell, are directly attributed to this reading.

Chapter 1 explains how to recognize an iSeries server during routine scans.

Chapter 2 shows how to create a list of valid user accounts on an iSeries server.

Chapter 3 shows the various methods to gain unplanned access to the server and to the assets it contains: Getting a command line, escalation of privileges, built-in tools to view and modify data.

Chapter 4 explains how to plant traps, bombs and Trojan horses triggered by unsuspecting parties or by system events.

Chapter 5 shows how to use the multiple command execution capabilities of the server to execute remote commands, create backdoors and reverse shells, and what common programming tools can be used in your scripts.

Chapter 6 explains how to use the iSeries server to investigate the network environment, connect to network resources, and attack workstation clients.

Chapter 7 shows what may happen when an AS/400 is used to host web sites and web applications.

In chapter 8 we will cover our tracks and manipulate the various system and audit logs.

Chapter 9 touches upon the possible vulnerabilities of commonly found iSeries security applications that use the security APIs provided by IBM.

To keep the book on schedule, I intentionally left out some topics, like SNA based vulnerabilities and physical security. Please fill up the survey on the web site, at <http://www.venera.com> to let me know what topics should in your opinion be added or expanded in future editions.

Chapter 1: Server footprinting

The first action a hacker does when given access to your network is reconnaissance. The action of mapping the network and the servers is critical for evaluation of the possible attack vectors, for finding the soft spots of the enterprise, and for recognizing the assets available for plundering. A typical footprinting session will include network scanning to find responsive IP addresses, and port scanning of individual server ports to discover what services are available on the network. Not surprisingly, the iSeries uses some peculiar ports and particular responses that identify it easily.

1.1 Port scanning and banner grabbing

Besides the platform's particular banners which are listed further on in this chapter, there are a number of platform specific ports that may indicate an iSeries server.

Note that the system administrator may change most of the default ports.

Service name	Description	Port number
ddm	DDM server is used to access data via DRDA and for record level access.	446
As-svrmap	Port mapper returns the port number for the requested server.	449
As-admin-http	HTTP server administration.	2001
As-mtgctrlj	Management Central server is used to manage multiple AS/400s in a network.	5544
As-mtgctrl	Management Central server is used to manage multiple AS/400s in a network.	5555
As-central	Central server is used when a Client Access license is required and for downloading translation tables.	8470
As-database	Database server is used for accessing the AS/400 database.	8471
As-dtaq	Data Queue server allows access to the AS/400 data queues, used for passing data between applications.	8472
As-file	File Server is used for accessing any part of the AS/400 file system.	8473
as-netprt	Printer Server is used to access printers known to the AS/400.	8474
as-rmtcmd	Remote command server is used to send commands	8475

	from a PC to an AS/400 and for program calls.	
as-signon	Sign-on server is used for every Client Access connection to authenticate users and to change passwords.	8476
as-usf	Ultimedia facilities are used for multimedia data.	8480

Table 1: Common non-secure ports

The following table shows port numbers for host servers and daemons that use Secure Sockets Layer (SSL):

Service name	Description	Port Number
ddm-ssl	DDM server is used to access data via DRDA and for record level access.	447, 448
telnet-ssl	Telnet server.	992
as-admin-https	HTTP server administration.	2010
as-mgtctrl-ss	Management Central server is used to manage multiple AS/400s in a network.	5566
as-mgtctrl-cs	Management Central server is used to manage multiple AS/400s in a network.	5577
as-central-s	Central server is used when a Client Access license is required and for downloading translation tables.	9470
as-database-s	Database server is used for accessing the AS/400 database.	9471
as-dtaq-s	Data Queue server allows access to the AS/400 data queues, used for passing data between applications.	9472
as-file-s	File Server is used for accessing any part of the AS/400 file system.	9473
as-netprt-s	Printer Server is used to access printers known to the AS/400.	9474
as-rmtcmd-s	Remote command server is used to send commands from a PC to an AS/400 and for program calls.	9475
As-signon-s	Sign-on server is used for every Client Access connection to authenticate users and to change passwords.	9476

Table 2: Common secure ports

More information including a list of iSeries Access for Windows functions and the servers used by those functions can be found here:

http://www-912.ibm.com/n_dir/nas4apar.NSF/c79815e083182fec862564c00079d117/fcc664db54c4c549862568720047b5fd?OpenDocument&Highlight=2,ii12227

There are many useful port scanning tools, but for our purposes we can use netcat to scan an iSeries server from the network it resides on. Netcat is an extremely useful utility that is used in several places throughout this book. It can even run on the iSeries itself to create a reverse shell available on the internet – as shown in chapter 5, "Remote reverse shell using netcat".

```
$ nc -v -z -w 1 as400.victim.com 1-100 | grep "open"
```

```
as400.victim.com [192.168.1.1] 80 (http) open
as400.victim.com [192.168.1.1] 25 (smtp) open
as400.victim.com [192.168.1.1] 23 (telnet) open
as400.victim.com [192.168.1.1] 21 (ftp) open
```

Telnet

The iSeries server supports a special type of Telnet stream called TN5250. To get full benefit from the 5250 features you need a special Telnet client. There are easy to get and inexpensive 5250 clients, such as MochaSoft (found at www.mochasoft.dk).

Of course, if you have a legal user name due to your position in the server owner's company, then you may already have a Telnet client on your workstation.

A regular iSeries sign-on screen looks like this:

Sign on		System :	S0011223
		Subsystem :	QINTER
		Display :	QPDEV00001
User :	_____		
Password :	_____		
Program/procedure :	_____		
Menu :	_____		
Current library :	_____		

(C) COPYRIGHT IBM CORP. 1980, 1999.

Figure 1: Sample iSeries log in screen

Let's explain the screen layout:

The top right corner displays the server's APPN network name, the subsystem name, and the name assigned to your terminal session. This trio is an iSeries fingerprint. The system administrator can hide the program, menu, and library fields, in chapter 3 we will demonstrate what can happen if those input fields are not hidden.

NOTE

A regular windows or UNIX telnet client can also be used with limited functionality to work with iSeries menus and programs.

FTP

Netcat can be successfully used to grab an FTP banner, enabling us see from the very beginning that we're dealing with an AS400 server.

```
$ echo quit | nc -v as400.victim.com 21
as400.victim.com [198.162.0.1] 21 (ftp) open
220-QTCP at S0011223.VICTIM.COM.
220 Connection will close if idle more than 5 minutes.
221 QUIT subcommand received.
```

Those 220 lines are a telltale sign of an iSeries server, especially the "QTCP at ..." string. If you have a valid user profile on the AS400 and are able to log in (perhaps as an anonymous user), then the server can be made to cough up more disclosing information.

```
C:\> ftp as400.victim.com
Connected to as400.victim.com.
220-QTCP at S0011223.VICTIM.COM.
220 Connection will close if idle more than 5 minutes.
ftp> quote syst
215 OS/400 is the remote operating system. The TCP/IP version is
"V4R4M0".
```



Countermeasure:

The first 220 line originates in message TCP120D from the QTCP/QTCPMSGF message file, and the variable fields in it representing the user who runs the process and the server's IP address cannot be changed. I do not recommend changing the user to anything other than QTCP, because such a change can have unforeseen consequences. Besides, most if not all damaging attacks require the hacker to have a valid account (user profile), so do not stay awake at night because the system reveals its OS to non-authenticated users.

However, the exposure resulting from the "quote syst" FTP command is more serious: There are differences between the OS levels. Some may be quite meaningful in directing an attacker towards the most effective attack venues. The message ID is TCP1222 from QTCP/QTCPMSGF.

HTTP

Again, netcat is used to grab the service banner. "IBM-HTTP-Server/1.0" is only used in the AS400 original HTTP server context.

```
$ echo GET / | nc -v as400.victim.com 80
HTTP/1.1 200 Document follows
Server: IBM-HTTP-Server/1.0
Date: Thu, 27 Feb 2003 17:16:03 GMT
Content-Location: index.html
Connection: close
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 305
Last-Modified: wed, 01 Dec 1999 13:01:53 GMT
<html>
. . .
```


If the HTTP server you attempt to survey is connected to the Internet, an easy way is to use HTTP discovery services, such as Netcraft at www.netcraft.com (Read about AS400 HTTP server vulnerabilities in chapter 8).

SMTP

The AS400 server can be used as an enterprise email server, providing both SMTP and POP3 protocols. Both protocols can be used to verify the server type.

Revealing SMTP banners

Let us use Telnet on port 25 to see how the iSeries SMTP server responds.

```
$ telnet as400.victim.com 25
220 s0011223.VICTIM.COM running IBM AS/400 SMTP V05R01M00 on Thu, 27
Feb 2003 17:56:18 +0200.

help
214- valid commands are:
214- HELO MAIL RCPT DATA RSET QUIT NOOP
214- HELP VRFY
214- Commands not valid are:
214- SEND SOML SAML TURN
214- Mail forwarding handled by this server.
214- s0011223.VICTIM.COM is running the OS/400 operating system.
214- For more information, enter HELP <topic>.
214- For local information contact POSTMASTER @ s0011223.VICTIM.COM.
214 End of help information.
quit
221 s0011223.VICTIM.COM Service closing transmission channel.
```



Countermeasures:

The first 220 line originates in message TCP120D from the QTCP/QTCPMSGF message file, and the variable fields in it representing the user who runs the process and the server's IP address cannot be changed. I do not recommend changing the user to anything other than QTCP, because such a change can have unforeseen consequences.

SMTPScan tool

SMTPScan is a tool to find out which MTA is used, by sending several "special" SMTP requests and comparing the error codes returned with those in the fingerprint database. It does not take into account banners and other text information that cannot be trusted, only error codes.

This tool can be downloaded from: <http://www.greyhats.org/ouutils/smtpscan/>

Moreover, a document has been written describing the method implemented in SMTPScan that can be downloaded (PDF format) at:

http://www.greyhats.org/ouutils/smtpscan/remote_smtp_detect.pdf

Add the following line to the fingerprint file of SMTPScan:

```
IBM AS/400 SMTP
V05R01M00:503:501:250:501:250:501:250:501:250:501:214:502:502:250:500
```



Countermeasures:

Do not enable SMTP if you don't have to. If you have an internal mail server such as Exchange or Domino, consider using their SMTP gateways for outgoing email from AS400 applications, even at the expense of buying emailing software which is not very expensive for the AS400.

POP3

Here is what a POP3 session with an AS400 server looks like:

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

The CPF2204 code message ID is a sure sign we're dealing with an AS400. We'll elaborate on POP3, CPF2204 and similar protocols in Chapter 2.



Countermeasures:

If you were in doubt regarding SMTP, you shouldn't be in doubt regarding POP3. Get a real mail server for your company. As we'll see later on, POP3 is not protected by any exit programs, and provides the best venue for an intruder to enumerate your users. The POP3 server also creates potential content security problems – read about it in chapter 3. If you already have another mail server – disable POP3 immediately.

SNMP

The iSeries supports SNMP since OS/400 version 3.1. SNMP can be a great tool to manage your network and your servers. However, when improperly configured, SNMP provides a hacker with foot-printing information. SNMP can also reveal a lot of valuable information about your server and network, such as the list of all clients currently connected to the server, communication configurations and definitions, and a list of hardware on your server. Read more about SNMP disclosures in chapter 6.

To extract the following sample SNMP report, SNMPWALK (by Cyneric) was used on a default, out-of-the-box iSeries installation. The list has been edited for brevity, and the interesting parts have been highlighted.

```
C:\> snmpwalk 192.168.0.1 public .1.3

.iso.3.6.1.2.1.1.1.0 = "IBM OS/400 V5R1M0"
.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: (39659506) 4 days, 14:09:55.06
.iso.3.6.1.2.1.1.4.0 = ""
.iso.3.6.1.2.1.1.5.0 = "S0011223.VICTIM.CORP"
.iso.3.6.1.2.1.1.6.0 = ""
.iso.3.6.1.2.1.1.7.0 = 72
.iso.3.6.1.2.1.2.1.0 = 2
.iso.3.6.1.2.1.2.2.1.1.1 = 1
.iso.3.6.1.2.1.2.2.1.1.2 = 2
.iso.3.6.1.2.1.2.2.1.2.1 = "*LOOPBACK "
.iso.3.6.1.2.1.2.2.1.2.2 = "ETHLINE "
.iso.3.6.1.2.1.2.2.1.3.1 = 1
<. . . . >
```



Countermeasures:

Do you really use SNMP? If the answer is no, then SNMP should not be automatically started with the rest of the TCP/IP servers. The following command will remove SNMP from the autostart list: CHGSNMPA AUTOSTART(*NO) . This method will not work when using an explicit start-all command, such as STRTCPSVR SERVER(*ALL), so in addition you should completely remove the PUBLIC community string.

On the other hand, if you do use SNMP, take your time to configure it properly:

- Delete the PUBLIC community and create another, non-trivial community, with proper manager IP addresses, using either Operations Navigator, or option 2 of the CFGTCPSNMP command.
- To define the authentication event trapping use the CHGSNMPA command.
- Log at least the SNMP traps, and the set requests.

See appendix A for detailed instructions for disabling SNMP on your AS400 server.

Summary

The AS/400 server supports a variety of TCP network services. Some are proprietary to the platform and use proprietary ports, such as the Management Central service on ports 5566 and 5577. Others are well known and widely used TCP services whose responses and banners disclose the fact that the server we're dealing with is an IBM AS/400.