

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.....	21
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.....	83
4.3 Hijacking terminal devices	85
4.4 Hijacking printed output.....	86
4.5 Adding payload to events	88
Manipulating command objects	88
Event exit programs	92
Message queue trapping	93
DB2 trigger programs.....	94
4.6 Hacking work management	94
Scheduled jobs	94
Subsystems	95
4.7 Hacking communications	97
Creating a DRDA Transaction Processing Program.....	97
Changing INETD.....	98
Adding unplanned TCP/IP services.....	99
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>	175
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>	181
<i>Appendix C: Client Access Express</i>	185
<i>Appendix D: References</i>	186
Web sites	186
Printed and electronic Books	188
iSeries Security applications and vendors	189
<i>Index</i>	191

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)	80
Figure 59: Change initial program in a user profile (native mode)	80
Figure 60: Display program information.....	81
Figure 61: Display menu attributes	83
Figure 62: Work with message file of menu options	84
Figure 63: Change AS400 menu options	84
Figure 64: Display subsystem's sign-on screen	86
Figure 65: Work with LPR output queue	87
Figure 66: Add new printer port in Windows.....	87
Figure 67: Add LPR printer in Windows	88
Figure 68: Display command information	89
Figure 69: Display command information, continued	90
Figure 70: Work with event exit point registration.....	93
Figure 71: Display subsystem description command output.....	95
Figure 72: Display routing entry.....	96
Figure 73: Work with Relational databases.....	97
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.....	99
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