

CONTENTS

About the Author	17
Forward	18
Introduction	20
But How Likely is the Threat, Really?	20
Why Would I Write Such a Book!?	21
Intended Audience.....	22
What This Book Is/Isn't	22
Requirements.....	23
Conventions	23
Part I - SCADA Overview	25
Chapter 1: What is a SCADA System?	26
SCADA System Evolution, Definitions, and Basic Architecture	26
<i>SCADA Evolution</i>	27
<i>SCADA Definitions</i>	29
<i>SCADA System Architecture</i>	31
SCADA Protocols	35
<i>The MODBUS Model</i>	36
<i>The DNP/DNP3 Model</i>	38
<i>UCA 2.0 and IEC61859</i>	40
<i>Controller Area Network</i>	42
<i>Control and Information Protocol</i>	44
<i>DeviceNet</i>	46
<i>ControlNet</i>	48
<i>EtherNet/IP</i>	50
<i>FFB</i>	52
<i>Profibus</i>	54
<i>OPC</i>	56
<i>ICCP</i>	58
SCADA Applications	60
SCADA in the Industry.....	61
<i>Petroleum Refining</i> <i>Nuclear Power Generation</i>	62
<i>Nuclear Power Generation</i>	63
<i>Conventional Electric Power Generation</i>	64
<i>Petroleum Wellhead Pump Control</i>	65
<i>Water Purification System</i>	66
<i>Crane Control</i>	67

Chemical Plants..... 68
Benzene Production 69
Embedded Systems 70
SCADA in the Corporation 71
Summary 72

Chapter 2: Critical Infrastructure Directives 73

Classifying Attacks and Threats 75
What is a Vulnerability? 75

SCADA System Security Issues Overview 79
SCADA and IT Convergence 80
Conventional IT Security and Relevant SCADA Issues 80

Part II - Reconnaissance 82

Chapter 3: Footprinting SCADA Environments..... 83
What Is Footprinting? 83
Footprinting Techniques 83
Publically Available Information 83
 Company Web Pages..... 84
 Related Organizations 84
 Google 86
 Whois..... 88
 Sam Spade 88
Footprinting Countermeasures 88
Summary 90

Chapter 4: Scanning SCADA Systems 91
Determining If the System Is Alive 91
Determining Which Services Are Running or Listening 92
Scan Types..... 93
Identifying TCP and UDP Services Running 95
Port Scanners 96
 NMap..... 96
 Netscan Tools Pro..... 97
 SuperScan 98
Port Scanning Breakdown..... 99
Common SCADA Network Ports..... 99
Detecting the Operating System 100
Active Stack Fingerprinting 100
Passive Stack Fingerprinting 100
Scanning Countermeasures 100
Summary 102

Chapter 5: Enumeration	103
Basic Banner Grabbing.....	103
Netcat.....	103
Enumerating Services	104
<i>NetBIOS Enumeration</i>	<i>104</i>
Net view	105
Nbtstat	105
Nltest.....	105
Netviewx	106
GFI LANGuard.....	106
<i>SNMP Enumeration</i>	<i>107</i>
Snmputil	107
SolarWinds	108
GFI LANGuard.....	108
<i>Active Directory Enumeration.....</i>	<i>109</i>
Idp	109
Null Sessions	110
Net use	110
Dumpsec.....	111
Enum	111
Nete.....	112
SuperScan.....	112
Enumeration Countermeasures.....	113
Defeating "RestrictAnonymous=1"	115
User2sid	115
Sid2user.....	115
Userinfo.....	116
Userdump.....	116
Getacct	116
walksam	117
Summary.....	117

Part V - The SCADA Network 118

Chapter 6: Firewalls.....	119
Firewall Architecture.....	119
Firewall Identification	121
<i>Direct Scanning.....</i>	<i>121</i>
<i>Route Tracing.....</i>	<i>122</i>
<i>Banner Grabbing</i>	<i>122</i>
Advanced Firewall Discovery	123
<i>Deduction with Nmap.....</i>	<i>123</i>
<i>Port Identification.....</i>	<i>123</i>

- Scanning Through Firewalls..... 125
 - Raw Packet Transmissions* 125
 - Firewalk** 125
 - Source Port Scanning* 126
- Packet Filtering..... 126
 - Liberal ACLs*..... 126
 - Deadly ICMP*..... 127
 - ICMP and UDP Tunneling*..... 127
 - Checkpoint?* 128
- Application Proxy Vulnerabilities 128
 - Hostname: localhost* 128
 - Unauthenticated External Proxy Access*..... 129
- Summary 130
- Chapter 7: Remote Modem and VPN Connectivity 131**
- Preparing to Dial Up..... 131
 - Phone Number Footprinting* 131
- War-Dialing 132
 - Hardware* 132
 - Legal Issues* 133
 - Peripheral Costs* 134
- Software 135
 - TonLoc*..... 135
 - TonLoc Batch Files*..... 135
 - THC-Scan*..... 136
 - PhoneSweep*..... 137
 - Carrier Exploitation*..... 138
- Brute-force Scripting 139
 - Low Hanging Fruit*..... 139
 - Single Authentication with Unlimited Attempts* 139
 - Single Authentication with Limited Attempts* 139
 - Dual Authentication with Unlimited Attempts* 140
 - Dual Authentication with Limited Attempts* 140
- Virtual Private Network (VPN) Hacking..... 143
- Summary 145
- Chapter 8: Network Devices and Protocols 146**
- Discovery 146
- Detection..... 147
- Profiling..... 149
 - Dig*..... 149
 - Traceroute*..... 150
 - IP Lookup*..... 151

Autonomous System Lookup	152
<i>Normal Traceroute</i>	152
<i>Traceroute with ASN Information</i>	153
<i>Show IP BGP</i>	153
Service Detection	154
<i>Nmap</i>	154
<i>Operating System Identification</i>	156
<i>Cisco Banner Grabbing and Enumeration</i>	157
Network Vulnerability.....	157
<i>Phenoelit</i>	157
OSI Layer 1	157
OSI Layer 2	159
<i>Detecting Layer 2 Media</i>	160
Sniffing	160
Switch Sniffing.....	162
<i>ARP Redirect (ARP Poisoning)</i>	163
<i>Broadcast Sniffing</i>	164
<i>VLAN Jumping</i>	165
<i>Internetwork Routing Protocol Attack Suite (IRPAS) and Cisco Discovery Protocol (CDP)</i>	167
<i>Spanning Tree Protocol (STP) Attacks</i>	169
<i>VLAN Trunking Protocol (VTP) Attacks</i>	171
OSI Layer 3	173
<i>TCP Sequence Number Prediction</i>	173
<i>Tcpdump</i>	174
<i>Dsniff</i>	174
<i>Ettercap</i>	175
Misconfigurations	176
<i>Read/Write MIB</i>	176
<i>Cisco Weak Encryption</i>	177
<i>TFTP Downloads</i>	178
<i>Configuration Analyzers</i>	178
RATS	178
Nipper	179
Route Protocol Hacking	181
<i>RIP Spoofing</i>	181
<i>Interior Gateway Routing Protocol (IGRP)</i>	182
<i>Open Shortest Path First (OSPF)</i>	182
<i>Border Gateway Protocol (BGP)</i>	183
<i>Spoofed BGP Packet Injection</i>	185
Management Protocol Hacking	186
<i>SNMP Request and Trap Handling</i>	186
Summary.....	187

Chapter 9: SCADA End-Devices (RTUs, PLCs, and IEDs) 188

- Remote Connectivity 188
 - Command Line Interface (CLI)*..... 188
 - Web-Based Management Interface*..... 190
- Denial of Service (DoS) 192
 - Insufficient Thresholds and Safeguards* 192
- SCADA Protocol and Data Transfer Hacking..... 195
 - Modbus* 195
 - Fieldbus*..... 198
 - DNP/DNP3* 201
 - Profibus*..... 206
 - OPC* 210
 - ICCP*..... 213
- Hacking Serial Devices from IP 219
 - Record and Playback*..... 219
 - Control Function Bit Manipulation*..... 223

Chapter 10: Wireless 227

- An 802.1x Overview 227
- Wireless Footprinting..... 230
 - Equipment*..... 230
 - Cards..... 230
 - Antennas 232
 - GPS 234
- Discovery Software 236
 - NetStumbler*..... 236
 - Kismet* 238
 - Dstumbler* 239
 - Cain* 241
- Wireless Mapping 243
 - StumbVerter*..... 243
 - GPSMap* 244
 - JiGLE*..... 245
- Wireless Scanning and Enumeration..... 246
 - Wireless Sniffers*..... 246
 - Configuring Linux Wireless Cards for Promiscuous Mode..... 247
 - Mognet 247
 - Wireless Monitoring Tools* 248
 - Prism2dump 248
 - Tcpdump..... 248
 - Wireshark 249
 - Airfart 251
 - AiroPeek NX..... 253

WifiScanner	254
Identifying Wireless Network Defenses and Countermeasures	255
SSID	255
MAC Access Control	256
Gvoid11	256
Identifying WEP	257
Gaining Access (Hacking 802.11)	258
SSID	258
MAC Access Control	259
Attacks Against the WEP Algorithm	260
AirSnort	260
AirCrack	261
AirReplay	262
WLAN-Tools	263
DWEPCrack	264
WEPAttack	265
Cain	265
LEAP Attacks	267
Anwrap	267
Asleep	268
Attacks Against the WPA Algorithm	270
Bluetooth	273
Redfang	273
Bluewave	274
Wireless Denial of Service (DoS) Attacks	276
Additional Resources	278

Part III - SCADA Servers, Clients, and WebHMIs 280

Chapter 11: Windows	281
Overview	281
<i>What's Not Covered</i>	281
Remote Attacks (Unauthenticated)	282
<i>Password Guessing</i>	282
NetBIOS Auditing Tool (NAT)	282
Smbgrind	283
fgrind	283
<i>Eavesdropping SMB</i>	285
Kerbsniff/KerbCrack	285
LOphtcrack SMBCapture	286
SoopLM/BeatLM	286
SMBRelay	287
SMB Man-in-the-Middle (MITM) Attacks	287

Cain.....	288
<i>Examples of MS Service Specific Vulnerabilities.....</i>	290
<i>Windows Internet Service Implementations (Intro).....</i>	292
Local Attacks / Privilege Escalation (Authenticated).....	295
<i>Named Pipes Prediction.....</i>	295
PipeUpAdmin.....	296
<i>NETDDE Requests Run As System.....</i>	297
netddemsg.....	298
<i>Exploiting the Windows Debugger.....</i>	299
Debploit.....	299
xdebug.....	300
<i>Grabbing Password Hashes.....</i>	301
<i>Grabbing Cleartext Passwords from the LSA Cache.....</i>	302
<i>Previous Logon Cache Dump.....</i>	303
<i>Dumping SAM and Active Directory (AD) Passwords.....</i>	304
PwDump2.....	305
samdump.....	306
<i>Cracking Passwords.....</i>	307
John the Ripper.....	308
LOphtcrack.....	309
<i>Passing the Hash.....</i>	311
<i>LSA Secrets.....</i>	312
Isadump.....	312
<i>File Searching.....</i>	313
Find.....	313
Findstr.....	314
Grep for Windows.....	315
<i>Remote Control and Back Doors.....</i>	316
Rogue User Accounts.....	316
Netcat.....	317
Remote.exe.....	318
Rsetup.....	319
Wsremote.....	319
PsExec.....	320
VNC.....	321
PCAnywhere.....	323
Trojans and Botnets.....	325
<i>Terminal Services.....</i>	327
RDP Overview.....	327
ProbeTS.....	328
TSEnum.....	328
Terminal Services Manager (tsadmin).....	329

Enumerating Trusted Domains with TS Logon	329
Tsgrinder	330
Tscrack.....	332
Privilege Escalation.....	332
Eavesdropping.....	333
<i>Keystroke Logging</i>	334
<i>Trojans and Trojan Ginas</i>	335
Planting Trojans.....	338
SubSeven.....	339
Back Oriffice 2000 (BO2K)	339
Trojan Logon Screens	340
FakeGINA.....	341
<i>Packet Capturing / "Sniffing"</i>	343
Dsniff for Win32	343
Fsniff.....	344
Wireshark.....	344
Cain	346
Ettercap	348
<i>Port Redirection</i>	350
rinetd.....	350
Fpipe.....	350
<i>Rootkits and Covering Your Tracks</i>	351
Disabling Auditing	352
Clearing the Event Log.....	352
Hiding Files	353
Attrib +h	353
Alternate Data Streams	354
Elitewrap	355
Windows Root Kits	356
Windows Security	358
<i>Keeping Up with Patches</i>	359
Group Policy.....	360
IPSec	362
Runas.....	363
.NET Framework	364
Windows Firewall	366
The Encrypting File System (EFS)	367
Windows 2000.....	368
Windows XP Service Pack 2	371
Windows Server 2003	374
Summary.....	377
Chapter 12: UNIX.....	378

- Got Root? 378
 - Unix Overview* 378
 - Vulnerability Mapping* 381
- Remote Access vs. Local Access 382
- Remote Attacks (Unauthenticated) 383
 - Brute-force Attacks* 383
 - Brutus 384
 - THC-Hydra 384
 - TeeNet 385
 - SNMPbrute 385
 - TSGrind 386
 - Data-Driven Attacks*..... 388
 - Buffer Overflow Attacks 388
 - Format String Attacks 389
 - Input Validation Attacks 389
 - Integer Overflow and Integer Sign Attacks..... 390
 - Shells*..... 391
 - Operation X 391
 - Reverse Telnet and Back Channels..... 392
 - Common Remote Attacks* 394
 - FTP 394
 - Sendmail..... 394
 - Remote Procedure Call (RPC) 395
 - SNMP Buffer Overflow? 395
 - NFS..... 396
 - X Vulnerabilities..... 396
 - Domain Name Server (DNS) 397
 - DNS TSIG Overflow? 397
 - SSH Vulnerabilities..... 399
 - OpenSSL Overflow? 400
 - Apache..... 401
 - Promiscuous-Mode Vulnerabilities 403
- Local Attacks (Authenticated) 404
 - Password Composition*..... 405
 - Crack* 405
 - John the Ripper* 406
 - Local Buffer Overflow?*..... 408
 - Symlink*..... 409
 - Race Conditions*..... 411
 - Core File Manipulation*..... 412
 - Shared Libraries* 414
 - Kernel Vulnerabilities* 415

<i>System Misconfiguration</i>	416
<i>File and Directory Permissions</i>	418
SUID Root	419
After Hacking Root	420
Rootkits	420
Trojans	422
Sniffers	424
Log Cleaning	425
Kernel Rootkits	425
Rootkit Recovery	426
Summary	427
Chapter 13: WebHMI Hacking	428
Web Server Hacking	428
Sample Files	429
Source Code Disclosure	430
Canonicalization Attacks	431
Server Extensions	432
Buffer Overflows	433
Web Server Vulnerability Scanners	433
Whisker	433
Nikto	433
Web Application Hacking	434
Hacking with Google	435
Web Crawling	436
Wget	437
Offline Explorer Pro	437
Web Application Assessment	438
Achilles	440
Paros Proxy	441
SPIKE Proxy	441
WebProxy	442
Form Scalpel	442
FSMax	443
WASAT	443
SPIKE	444
NTLM Authorization Proxy Server	444
Web Application Security Scanners	445
WebInspect and SPI Toolkit	445
N-Stalker	447
Sanctum/Watchfire and AppScan/WebMX	449
Kavado ScanDo and InterDo	451
Common Web Application Vulnerabilities	452

<i>SQL Injection</i>	453
<i>Automated SQL Injection Tools</i>	454
SQLninja	454
SQLmap	455
<i>Cross-Site Scripting (XSS)</i>	456
<i>HTTP Response Splitting</i>	459
<i>Misuse of Hidden Tags</i>	460
<i>Server Side Includes (SSIs)</i>	461
Web 2.0 (Web Services)	462
WebHMI Safeguards	465
Summary	468
Chapter 14: Hacking the Data Historian	469
Microsoft SQL Server	469
<i>Newsgroup Searches</i>	470
<i>Default Port</i>	470
<i>SQLPing</i>	470
<i>Basic SQL Query Tools</i>	471
Query Analyzer	471
SqlDict	471
<i>Advanced SQL Hacking Tools</i>	472
Sqlbf	472
Sqlpoke	473
Custom ASP Pages	473
<i>Sniffing SQL Server Passwords</i>	474
<i>Source Disclosure from Web Servers</i>	475
<i>Known SQL Server Vulnerabilities</i>	476
<i>SQL Injection Attacks</i>	478
<i>Abusing SQL Extended Stored Procedures to Manipulate Windows 2000</i>	480
PI Database	481
<i>OPC using DCOM</i>	483
Database Security	486

Chapter 15: Dual Homed Systems – Don't Do It!..... 490

Part IV - Software Hacking..... 492

Chapter 16: Hacking Applications	493
Common Exploit Techniques	493
<i>Buffer Overflows</i>	493
Stack Buffer Overflows	496
Heap/BSS/Data Overflows	497
Format String Vulnerabilities	498
Off-by-One Errors	499

<i>Input Validation Attacks</i>	500
Canonicalization Attacks	501
Web Application and Database Attacks	501
Application Security	502
Summary	505
Chapter 17: Hacking the End-User	506
Network Client Vulnerabilities	506
<i>Malicious Web Pages</i>	507
Microsoft ActiveX	507
Java	507
JavaScript and Active Scripting	508
Cookies	508
Cross-Site Scripting (XSS)	508
Cross-Frame/Domain Vulnerabilities	509
The Local Machine Zone (LMZ)	509
The IFRAME Tag	509
HTML Help ActiveX Control	510
<i>SSL Attacks</i>	511
Homograph Attacks	512
<i>Email Hacking</i>	513
File Attachments	513
MIME Execution	514
Address Book Worms	515
Senna Spy Worm Generator 2000	516
<i>Writing Local Files</i>	517
Executing .chm Files Written to Temporary Internet Cache	518
Writing Data to the Telnet Client Log	519
<i>Reading Local Files</i>	520
Reading Local Files with MSScriptControl	521
<i>Invoking Outbound Client Connections</i>	522
Harvesting NTLM Credentials Using Telnet://	523
<i>Instant Messaging (IM)</i>	524
<i>Microsoft Internet Client Vulnerabilities</i>	525
GDI+ JPEG Processing Buffer Overflow (IE6 SP1)?	525
IE showModalDialog Cross-Zone Exploit	525
IE Improper URL Canonicalization	526
IE HTML HelpControl Local Execution	526
<i>Online Services</i>	527
Phishing	527
<i>What is Phishing?</i>	527
<i>Why is Phishing dangerous to SCADA networks?</i>	528
<i>Phishing Techniques</i>	529

- Spyware, Adware, and Spam 531
 - Common Insertion Techniques*..... 532
 - Autostart Exensibility Points..... 532
 - Web Browser Add-Ons 533
 - Blocking, Detecting and Cleaning Spyware and Adware* 535
- Malware 536
 - Malware Variants and Common Techniques* 537
 - Viruses and Worms 537
 - Rootkits and Back Doors..... 538
 - Hacker Defender..... 539
 - Other Common Rootkits..... 540
 - Bots and Zombies 541
 - Detecting and Cleaning Malware* 544
- Client-Side Security 547
- Summary 554

Part VI - Denial of Service (DoS) 555

- Chapter 18: Common DoS Attacks Techniques 556**
- Old-School DoS: Vulnerabilities..... 557
 - Oversized Packets..... 557
 - Fragmentation Overlap 558
 - Loopback Floods 558
 - Nukers 559
 - Extreme Fragmentation..... 559
 - NetBIOS/SMB 560
 - Combos..... 560
- Modern DoS: Capacity Depletion 561
 - Infrastructure-Layer DoS*..... 561
 - SYN Floods 561
 - UDP Floods 562
 - Amplification: Smurf and Fraggle 563
 - Districuted Denial of Service (DDoS) 564
 - DDoS Clients and Bots 565
 - Application-Layer DoS*..... 566
- Windows 2000/2003 Dos Attacks 567
 - TCP Connect Flooding* 567
 - Application Services-Level DoS Attacks*..... 568
 - LAN-Based DoS Attacks*..... 569
 - DDoS Zombies* 570
 - WinTrinoo..... 570
- Field Devices..... 571
- Countermeasures Against DoS..... 574

Summary.....	577
--------------	-----

Part VII - Operations Security..... 578

Chapter 19: User Security and Awareness..... 579

Hacking Human Nature.....	579
<i>Social Engineering</i>	579
<i>Profiling the Systems Administrator</i>	582
Policies and Procedures.....	585
Training	586

Chapter 20: SCADA Security Standards and Regulations..... 588

ISO/IEC 17799:2005 (BS 7799-2:2002, AS 7799).....	588
ISA-TR99.00.01-2004	591
ISA-TR99.00.02-2004	593
API 1164	596
AGA 12	598
GAO-040140T.....	600
NIST SPP ICS	602
NIST 800-14.....	604
NIST 800-26.....	605
NIST 800-37.....	606
NIST SP800-52.....	607
NIST 800-53.....	609
NIST 800-53A	610
FIPS 199.....	611
6 CFR Part 27.....	612
NERC CIP 002-009	613

Part VIV - Physical Security..... 624

Chapter 21: Electronic Access Control 625

<i>Defeating Single Factor RFID Access Control</i>	625
--	-----

Chapter 22: Physical Access 628

Removable Media.....	628
Replacing the Screensaver.....	629
Offline Attacks Against the SAM	630
<i>Nullifying the Administrator Password by Deleting the SAM</i>	631
<i>Injecting Hashes into the SAM with chntpw</i>	632
Implications for EFS.....	633
<i>Reading EFS-Encrypted Files Using the Recovery Agent Credentials</i>	633
Defeating Recovery Agent Delegation	634
Reading EFS-Encrypted Data with User Account Credentials	635

EFS Temporary File Data Retrieval..... 635

Part X - Appendixes 636