

CONTENTS

Foreword	xvii
Case Study: The Black Hat Hassle	xx
Acknowledgments	xxiii
Introduction	xxv

Part I Foundations

Case Study: eBay Surprise	2
1 Cisco Network Design Models and Security Overview	5
Cisco Network Design Models: A Security Perspective	7
The Flat Earth Model	7
The Star Model	9
The Two-Tier Model	10
The Ring Model	11
The Mesh and Partial Mesh Model	12
Network Security Zones	14
IDS Sensor Deployment Guidelines	17
Cisco Hierarchical Design and Network Security	18
The Core Layer	19
The Distribution Layer	20
The Access Layer	21
Summary	22
2 Cisco Network Security Elements	23
Common Cisco Device Security Features	24
Cisco Firewalls	27
Packet-Filtering Firewalls	27
Stateful Packet-Filtering Firewalls	28
Proxy Filters	29

PIX Firewall Failover	30
Types of Cisco Firewall Hardware	32
Cisco Secure IDS and Attack Prevention	33
Hardware Standalone IDS Sensors	34
Modular IDS Sensors	36
Cisco IOS IDS Software	37
Cisco PIX Firewalls as IDS Sensors	39
Cisco Traffic Anomaly Detector XT 5600	40
Cisco Secure IDS Management Consoles	41
Cisco VPN Solutions	42
IPSec	44
PPTP	46
Cisco AAA and Related Services	47
Overview of AAA Methodology	47
Cisco and AAA	48
Security Implications of Cisco Internetwork Design and Security Elements	52
Summary	56
3 Real-World Cisco Security Issues	57
Why Do Hackers Want to Enable Your Box?	58
What Attackers Gain	59
Cisco Appliances and Networks: an Attacker's Perspective	62
Attacking Network Protocols	66
Hiding Tracks and Forensics on Routers and Switches	67
Cisco Network Device Security Auditing and Penetration Testing Foundations	69
The Evaluation Process	70
Summary	71

Part II "I Am Enabled": Hacking the Box

Case Study: The One with a Nessus Report	74
4 Profiling and Enumerating Cisco Networks	77
Online Searching and "Cisco Googledorks"	78
Basic Searching	79
Searching Using Google Operators	81
Googling for Enable	82
Routing Enumeration	84
Autonomous System Discovery and Mapping: BGPv4 Interrogation	84
Internet Routing Registries, Route Servers, and Looking Glasses Querying	86

Mapping IP Addresses to Autonomous Systems	92
Enumerating an Autonomous System	95
Finding Autonomous Systems That Belong to an Organization.....	99
AS Path Enumeration, Building BGP Trees, and Finding Border Routers	101
Routing Domain Number Discovery and Network Mapping for IGPs	108
Mapping RIP, IGRP, and IRDP	108
Enumerating OSPF	114
Analyzing OSPF Enumeration Data	116
Summary	121
5 Enumerating and Fingerprinting Cisco Devices	123
Sniffing for Cisco-Specific Protocols	124
Dissecting CDP Frames	128
Passive Enumeration and Fingerprinting of Cisco Devices.....	133
Active Enumeration and Fingerprinting of Cisco Devices	135
Active Enumeration and Fingerprinting of Cisco Routers.....	136
Active Enumeration and Fingerprinting of Catalyst Switches	143
Active Enumeration and Fingerprinting of Other Cisco Appliances ..	149
Using IOS 11.X Memory Leak to Enumerate Remote Cisco Routers ..	156
Summary	170
6 Getting In from the Outside: Dead Easy	171
Password Attacks	172
Mass Guessing/Bruteforcing Attacks Against Open Cisco Telnet Servers.....	173
Password Guessing and Bruteforcing Attacks Against Other Open Cisco Services.....	180
SNMP Community Guessing, Exploitation, and Safeguards	189
Cisco SNMP Basics	189
SNMP Mass Scanning	193
SNMP Bruteforcing and Dictionary Attacks	196
SNMP Browsing and Cisco Device Reconfiguration	199
Command-Line Remote Cisco Device SNMP Manipulation—IOS Hosts	207
Command-Line Remote Cisco Device SNMP Manipulation—CatOS Switches	213
Exploiting TFTP Servers to Take Over Cisco Hosts	221
Enumerating TFTP Servers	221
Sniffing Out Cisco Configuration Files	223
Bruteforcing TFTP Servers to Snatch Configs	224
Cisco Device Wardialing	225
Cisco Router Wardialing 101: Interfaces, Configurations, and Reverse Telnet	225

Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions

	Discovering the Numbers to Dial In	228
	Getting into a Cisco Router or an Access Server	230
	Summary	234
7	Hacking Cisco Devices: The Intermediate Path	237
	A Primer on Protocol Implementation Investigation and Abuse:	
	Cisco SNMP Attacks	238
	SilverCreek	240
	SimpleTester and SimpleSleuth	243
	Oulu University PROTOS Project	247
	From SNMP Fuzzing to DoS and Reflective DDoS.....	251
	From SNMP Stress Testing to Nongeneric DoS	252
	Hidden Menace—Undocumented SNMP Communities and Remote Access	253
	Getting In via Observation Skills Alone	256
	Brief SNMPv3 Security Analysis	259
	A Primer on Data Input Validation Attack—Cisco HTTP Exploitation	260
	Basics of Cisco Web Configuration Interface	260
	Cisco IOS HTTP Administrative Access	263
	Cisco ATA-186 HTTP Device Configuration Disclosure.....	264
	VPN Concentrator HTTP Device Information Leakage	265
	Other Cisco HTTPd Flaws—a More Sophisticated Approach	265
	Cisco IOS 2GB HTTP GET Buffer Overflow Vulnerability.....	266
	Assessing Security of a Cisco Web Service	267
	SPIKE and Its Relatives	268
	The Peach Fuzzer	271
	Summary	272
8	Cisco IOS Exploitation: The Proper Way	273
	Cisco IOS Architecture Foundations	274
	Cisco IOS Memory Dissection	275
	An Exploitation Primer: IOS TFTP Buffer Overflow	281
	Defeating Check Heaps	284
	The Curse and the Blessing of IOS Reverse Engineering	291
	IOS Features and Commands That Can Be (Ab)used by Reverse Engineers	292
	A Minimalistic Reverse Engineering Arsenal	293
	Summary	295
9	Cracking Secret Keys, Social Engineering, and Malicious Physical Access	297
	Cisco Appliance Password Cracking	298
	Cracking Type-7 Passwords	298
	Cracking MD5 Password Hashes.....	301
	Social Engineering Attacks	304

Local Device Access	308
Local Router Password Reset or Recovery	308
Local Switch Password Reset or Recovery	310
Local PIX Firewall Password Reset or Recovery	313
Local Cisco VPN Concentrator Password Reset or Recovery	315
Summary	316
10 Exploiting and Preserving Access	317
Common Cisco Router, Switch, or Firewall Reconfigurations by Attackers	318
Is Anyone Here?	318
Covering Tracks	320
Looking Around	323
Using a Hacked IOS Router to Hide Tracks	327
Using a Hacked IOS Router or PIX Firewall to Allow Malicious Traffic Through	328
Using a Hacked IOS Router to Mirror, Capture, and Modify Bypassing Traffic	330
Sniffing Traffic from a Hacked PIX Firewall	332
Sniffing the Network Using a Cisco Catalyst Switch	333
(Ab)using Remote SPAN	336
The Secret CatOS Enable Engineer Mode	337
Further IOS Exploitation and Device Access Preservation	340
IOS Binary Patching: Myth and Reality	340
TCLing the Router for Fun and Profit	353
Summary	360
11 Denial of Service Attacks Against Cisco Devices	361
DoS Attack Motives	362
Types of DoS Attacks	363
Consumption of Resources	363
Disruption of Information Flow	364
Disruption of Communication	364
Cisco DoS Assessment Tools	364
Cisco Global Exploiter	365
Cisco TCP Test Tool	366
Well-Known Cisco DoS Vulnerabilities	367
Cisco Devices Generic DoS	367
ICMP Remote DoS Vulnerabilities	367
Malformed SNMP Message DoS Vulnerability	369
Examples of Specific DoS Attacks Against Cisco Routers	370
Cisco IOS Malformed IKE Packet Remote DoS Vulnerability	370
Cisco 44020 Bug	370

Examples of Specific DoS Attacks Against Catalyst Switches and Other Cisco Networking Devices	372
Cisco Catalyst Memory Leak DoS Vulnerability	372
Incorrect TCP Checksum Attack Disrupting Communication Through a PIX Firewall.	373
Cisco Broadband OS TCP/IP Stack DoS Vulnerability	373
Cisco Aironet AP1x00 Malformed HTTP GET DoS Vulnerability	374
Cisco Catalyst Nonstandard TCP Flags Remote DoS Vulnerability ...	375
Abusing Cisco Appliances for Nasty DDoS Deeds	376
Mass Cisco Pinging, the SNMP Way	376
Mass Cisco Pinging, the Telnet Way MK I	376
Mass Cisco Pinging, the Telnet Way MK II.	378
Mass Cisco Flood, the SNMP Way	379
DDoS Massive: Revenge of the Kiddies	382
Direct DDoS Attacks	382
Reflective DDoS Attacks	382
ihateperl.pl	383
drdos	383
Summary	390

Part III Protocol Exploitation in Cisco Networking Environments

Case Study: The Flying OSPF Hell	394
12 Spanning Tree, VLANs, EAP-LEAP, and CDP	397
Spanning Tree Protocol Exploitation	398
Inserting a Rogue Root Bridge	402
Modifying a Traffic Path Without Becoming Root	410
Recalculating STP and Data Sniffing	411
STP DoS Attacks	412
Exploiting VLANs	415
DTP Abuse	412
802.1q and ISL Exploitation	416
Double Tagging VLAN Hopping	419
Private VLAN Hopping	420
Making Unidirectional Attacks Bidirectional	421
VTP Exploitation	422
VLAN Query Protocol (VQP) Attacks	423
Lateral Means of Bypassing VLAN Segmentation	426
Cisco EAP-LEAP Cracking	431
EAP-LEAP Basics	432
EAP-LEAP Cracking	432

Attacking CDP	438
A Sneaky CDP Attack	438
Summary	440
13 HSRP, GRE, Firewalls, and VPN Penetration	443
HSRP Exploitation	444
GRE Exploitation	447
An MTU-Based Attack Against GRE.....	447
GRE Packet Injection	448
Cisco Firewall Penetration	453
Attacking PIX Protocol Fixups	453
Attacking PIX MailGuard	453
Attacking PIX FTP Fixup.....	454
TCP RESET Attacks Against PIX Firewalls.....	456
Cisco VPN Hacking	459
IPSec-Related Attacks	460
Cisco PPTP Hacking.....	467
Summary	470
14 Routing Protocols Exploitation	471
Introduction to Routing Attacks	472
Setting Up a Rogue Router	474
Attacking Distance-Vector Routing Protocols	474
Attacking RIP	475
Malicious Route Insertion via RIP.....	475
RIP Downgrading Attack	481
RIP MD5 Hash Cracking Attack.....	482
Attacking IGRP	486
Malicious Route Insertion via IGRP	487
Attacking EIGRP	488
Malicious Route Insertion via EIGRP	488
DoS Attacks Against EIGRP Networks.....	492
Attacking Authenticated EIGRP	494
Attacking Link State Routing Protocols	498
Malicious Route Insertion via OSPF	499
Becoming a Designated or Backup Designated OSPF Router	504
OSPF MD5 Hash Cracking Attack.....	506
Direct Attack Against an OSPF Router: The OoopSPF Exploit	507
Possible DoS Attacks Against OSPF	509
Attacking BGPv4	512
Malicious BGP Router Reconfiguration	513
Attack Scenarios for Malicious BGP Router Reconfiguration	516
BGP Router Masquerading Attack.....	519

Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions

Man-in-the-Middle Attacks Against BGP Routers	520
Cracking BGP MD5 Authentication.	522
Blind DoS Attacks Against BGP Routers	523
Summary	528

Part IV Appendixes

Case Study: The Epic Battle	530
A Network Appliance Security Testing Template	533
B Lab Router Interactive Cisco Auto Secure ConFIGuration Example	539
C Undocumented Cisco Commands	549
Index	593