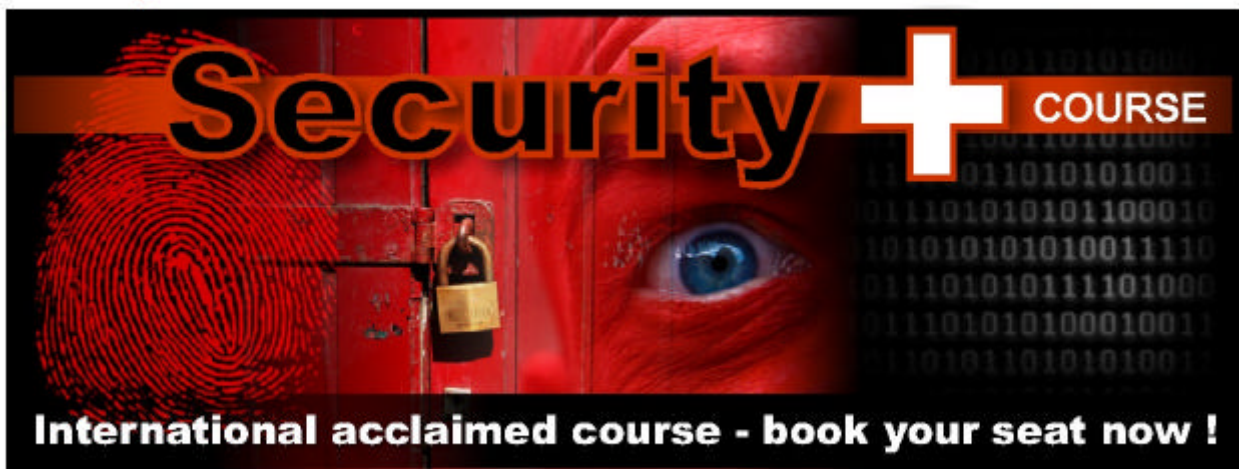


Security+

Course Content

CompTIA

26 - 30 July 2010

A banner for the Security+ course. The background is a collage of security-related images: a red fingerprint, a red padlock on a door, a blue eye, and binary code. The word "Security" is written in a large, bold, orange font with a black outline. A white plus sign is positioned to the right of "Security", and the word "COURSE" is written in a smaller, white, sans-serif font to the right of the plus sign. Below the banner, the text "International acclaimed course - book your seat now !" is written in a white, bold, sans-serif font.

Security+ COURSE

International acclaimed course - book your seat now !

www.infocure.co.za

+27 (0) 86 111 2221

info@infocure.co.za

CONTENTS

Acknowledgments	xxv
Preface	xxvii
Introduction	xxix

Part I	Security Concepts	1
Chapter 1	General Security Concepts	3
	The Security+ Exam	3
	Basic Security Terminology	6
	Security Basics	7
	Access Control	16
	Authentication	19
	Chapter Review	21
	Quick Tips	21
	Questions	22
	Answers	25
Chapter 2	Operational Organizational Security	27
	Policies, Standards, Guidelines, and Procedures	27
	The Security Perimeter	28
	Logical Access Controls	30
	Access Control Policies	30
	Social Engineering	34
	Phishing	35
	Vishing	36
	Shoulder Surfing	36
	Dumpster Diving	37
	Hoaxes	37
	Organizational Policies and Procedures	37
	Security Policies	38
	Privacy	43
	Service Level Agreements	44
	Human Resources Policies	44
	Code of Ethics	46
	Chapter Review	47
	Questions	47
	Answers	50

Chapter 3	Legal Issues, Privacy, and Ethics	53
	Cybercrime	54
	Common Internet Crime Schemes	55
	Sources of Laws	56
	Computer Trespass	56
	Significant U.S. Laws	57
	Payment Card Industry Data Security Standards (PCI DSS)	59
	Import/Export Encryption Restrictions	60
	Digital Signature Laws	63
	Digital Rights Management	65
	Privacy	66
	U.S. Privacy Laws	66
	European Laws	67
	Ethics	68
	SANS Institute IT Code of Ethics	69
	Chapter Review	71
	Questions	71
	Answers	73

Part II Cryptography and Applications 75

Chapter 4	Cryptography	77
	Algorithms	78
	Hashing	81
	SHA	82
	Message Digest	84
	Hashing Summary	86
	Symmetric Encryption	86
	DES	87
	3DES	89
	AES	90
	CAST	91
	RC	91
	Blowfish	94
	IDEA	94
	Symmetric Encryption Summary	95
	Asymmetric Encryption	95
	RSA	96
	Diffie-Hellman	97
	ElGamal	98
	ECC	98
	Asymmetric Encryption Summary	99
	Steganography	99

	Cryptography Algorithm Use	100
	Confidentiality	100
	Integrity	101
	Nonrepudiation	101
	Authentication	101
	Digital Signatures	102
	Key Escrow	102
	Cryptographic Applications	103
	Chapter Review	104
	Questions	104
	Answers	107
Chapter 5	Public Key Infrastructure	109
	The Basics of Public Key Infrastructures	109
	Certificate Authorities	112
	Registration Authorities	113
	Local Registration Authorities	116
	Certificate Repositories	116
	Trust and Certificate Verification	116
	Digital Certificates	120
	Certificate Attributes	121
	Certificate Extensions	123
	Certificate Lifecycles	124
	Centralized or Decentralized Infrastructures	130
	Hardware Storage Devices	131
	Private Key Protection	132
	Key Recovery	133
	Key Escrow	135
	Public Certificate Authorities	136
	In-house Certificate Authorities	137
	Outsourced Certificate Authorities	138
	Tying Different PKIs Together	139
	Trust Models	140
	Chapter Review	146
	Questions	147
	Answers	152
Chapter 6	Standards and Protocols	155
	PKIX/PKCS	157
	PKIX Standards	158
	PKCS	162
	Why You Need to Know	163
	X.509	164
	SSL/TLS	165
	ISAKMP	167

CMP	168
XKMS	169
S/MIME	171
IETF S/MIME v3 Specifications	172
PGP	173
How PGP Works	173
Where Can You Use PGP?	174
HTTPS	174
IPsec	175
CEP	175
FIPS	175
Common Criteria (CC)	176
WTLS	176
WEP	177
WEP Security Issues	177
ISO/IEC 27002 (Formerly ISO 17799)	177
Chapter Review	178
Questions	179
Answers	181

Part III Security in the Infrastructure **183**

Chapter 7	Physical Security	185
	The Security Problem	185
	Physical Security Safeguards	188
	Walls and Guards	188
	Policies and Procedures	189
	Access Controls and Monitoring	191
	Environmental Controls	193
	Authentication	194
	Chapter Review	197
	Questions	197
	Answers	199
Chapter 8	Infrastructure Security	201
	Devices	201
	Workstations	202
	Servers	204
	Network Interface Cards	205
	Hubs	206
	Bridges	206
	Switches	206
	Routers	208
	Firewalls	209

Wireless	212
Modems	214
Telecom/PBX	215
RAS	215
VPN	216
Intrusion Detection Systems	216
Network Access Control	216
Network Monitoring/Diagnostic	217
Mobile Devices	218
Media	219
Coaxial Cable	219
UTP/STP	219
Fiber	221
Unguided Media	222
Security Concerns for Transmission Media	224
Physical Security	224
Removable Media	225
Magnetic Media	225
Optical Media	227
Electronic Media	228
Security Topologies	229
Security Zones	229
Telephony	233
VLANs	233
NAT	235
Tunneling	236
Chapter Review	236
Questions	237
Answers	239
Chapter 9 Authentication and Remote Access	241
The Remote Access Process	241
Identification	242
Authentication	243
Authorization	247
IEEE 802.1x	247
RADIUS	248
RADIUS Authentication	248
RADIUS Authorization	250
RADIUS Accounting	250
DIAMETER	250
TACACS+	251
TACACS+ Authentication	251
TACACS+ Authorization	253
TACACS+ Accounting	253

	L2TP and PPTP	254
	PPTP	254
	PPP	256
	CHAP	256
	PAP	257
	EAP	257
	L2TP	257
	NT LAN Manager	258
	Telnet	258
	SSH	258
	IEEE 802.11	260
	VPNs	260
	IPsec	261
	Security Associations	262
	IPsec Configurations	262
	IPsec Security	265
	Vulnerabilities	268
	Chapter Review	269
	Questions	270
	Answers	272
Chapter 10	Wireless Security	275
	Wireless Networking	275
	Mobile Phones	276
	Bluetooth	279
	802.11	281
	Chapter Review	289
	Questions	289
	Answers	292
Part IV	Security in Transmissions	295
Chapter 11	Intrusion Detection Systems	297
	History of Intrusion Detection Systems	298
	IDS Overview	299
	Host-based IDSs	300
	Advantages of HIDSs	304
	Disadvantages of HIDSs	305
	Active vs. Passive HIDSs	306
	Resurgence and Advancement of HIDSs	306
	PC-based Malware Protection	307
	Antivirus Products	307
	Personal Software Firewalls	310
	Pop-up Blocker	312
	Windows Defender	313

	Network-based IDSs	315
	Advantages of a NIDS	319
	Disadvantages of a NIDS	319
	Active vs. Passive NIDSs	320
	Signatures	320
	False Positives and Negatives	322
	IDS Models	322
	Intrusion Prevention Systems	323
	Honeypots and Honeynets	325
	Firewalls	327
	Proxy Servers	327
	Internet Content Filters	328
	Protocol Analyzers	329
	Network Mappers	331
	Anti-spam	331
	Chapter Review	333
	Questions	334
	Answers	337
Chapter 12	Security Baselines	339
	Overview Baselines	339
	Password Selection	340
	Password Policy Guidelines	340
	Selecting a Password	342
	Components of a Good Password	343
	Password Aging	343
	Operating System and Network Operating System Hardening	344
	Hardening Microsoft Operating Systems	345
	Hardening UNIX- or Linux-Based Operating Systems	347
	Network Hardening	363
	Software Updates	364
	Device Configuration	364
	Ports and Services	366
	Traffic Filtering	368
	Application Hardening	370
	Application Patches	371
	Patch Management	371
	Web Servers	374
	Mail Servers	377
	FTP Servers	379
	DNS Servers	379
	File and Print Services	380
	Active Directory	381
	Group Policies	382
	Security Templates	384

	Chapter Review	385
	Questions	386
	Answers	388
Chapter 13	Types of Attacks and Malicious Software	391
	Avenues of Attack	391
	The Steps in an Attack	392
	Minimizing Possible Avenues of Attack	394
	Attacking Computer Systems and Networks	394
	Denial-of-Service Attacks	394
	Backdoors and Trapdoors	398
	Null Sessions	398
	Sniffing	399
	Spoofing	400
	Man-in-the-Middle Attacks	403
	Replay Attacks	404
	TCP/IP Hijacking	405
	Attacks on Encryption	405
	Address System Attacks	406
	Password Guessing	407
	Software Exploitation	409
	Malicious Code	409
	War-Dialing and War-Driving	416
	Social Engineering	417
	Auditing	417
	Chapter Review	418
	Questions	419
	Answers	422
Chapter 14	E-Mail and Instant Messaging	425
	Security of E-Mail	425
	Malicious Code	426
	Hoax E-Mails	428
	Unsolicited Commercial E-Mail (Spam)	429
	Mail Encryption	431
	Instant Messaging	435
	Chapter Review	438
	Questions	438
	Answers	441
Chapter 15	Web Components	443
	Current Web Components and Concerns	444
	Protocols	444
	Encryption (SSL and TLS)	444
	The Web (HTTP and HTTPS)	451
	Directory Services (DAP and LDAP)	452

File Transfer (FTP and SFTP)	454
Vulnerabilities	455
Code-Based Vulnerabilities	455
Buffer Overflows	456
Java and JavaScript	457
ActiveX	459
Securing the Browser	461
CGI	461
Server-Side Scripts	462
Cookies	462
Signed Applets	465
Browser Plug-ins	466
Application-Based Weaknesses	467
Open Vulnerability and Assessment Language (OVAL)	468
Chapter Review	469
Questions	469
Answers	472

Part V Operational Security 473

Chapter 16 Disaster Recovery and Business Continuity 475

Disaster Recovery	475
Disaster Recovery Plans/Process	476
Backups	478
Utilities	487
Secure Recovery	487
High Availability and Fault Tolerance	488
Chapter Review	488
Questions	489
Answers	491

Chapter 17 Risk Management 493

An Overview of Risk Management	493
Example of Risk Management at the International Banking Level	494
Key Terms for Understanding Risk Management	494
What Is Risk Management?	495
Business Risks	497
Examples of Business Risks	497
Examples of Technology Risks	498
Risk Management Models	498
General Risk Management Model	499
Software Engineering Institute Model	502
Model Application	502

	Qualitatively Assessing Risk	502
	Quantitatively Assessing Risk	505
	Qualitative vs. Quantitative Risk Assessment	507
	Tools	508
	Chapter Review	509
	Questions	509
	Answers	511
Chapter 18	Change Management	513
	Why Change Management?	514
	The Key Concept: Separation (Segregation) of Duties	515
	Elements of Change Management	517
	Implementing Change Management	519
	The Purpose of a Change Control Board	520
	Code Integrity	522
	The Capability Maturity Model Integration	522
	Chapter Review	523
	Questions	523
	Answers	526
Chapter 19	Privilege Management	529
	User, Group, and Role Management	530
	User	530
	Groups	532
	Role	532
	Password Policies	533
	Domain Password Policy	534
	Single Sign-On	535
	Centralized vs. Decentralized Management	536
	Centralized Management	536
	Decentralized Management	537
	The Decentralized, Centralized Model	538
	Auditing (Privilege, Usage, and Escalation)	538
	Privilege Auditing	538
	Usage Auditing	539
	Escalation Auditing	540
	Logging and Auditing of Log Files	541
	Common Logs	541
	Periodic Audits of Security Settings	542
	Handling Access Control (MAC, DAC, and RBAC)	543
	Mandatory Access Control (MAC)	543
	Discretionary Access Control (DAC)	545
	Role-based Access Control (RBAC)	546
	Rule-based Access Control (RBAC)	546
	Account Expiration	547

	Permissions and Rights in Windows Operating Systems	547
	Chapter Review	549
	Questions	550
	Answers	552
Chapter 20	Computer Forensics	553
	Evidence	554
	Standards for Evidence	554
	Types of Evidence	554
	Three Rules Regarding Evidence	555
	Collecting Evidence	555
	Acquiring Evidence	556
	Identifying Evidence	558
	Protecting Evidence	558
	Transporting Evidence	558
	Storing Evidence	558
	Conducting the Investigation	559
	Chain of Custody	560
	Free Space vs. Slack Space	561
	Free Space	561
	Slack Space	561
	Message Digest and Hash	561
	Analysis	562
	Chapter Review	563
	Questions	564
	Answers	566
Part VI	Appendixes	567
Appendix A	About the CD	569
	System Requirements	569
	LearnKey Online Training	569
	Installing and Running MasterExam	569
	MasterExam	570
	Electronic Book	570
	Help	570
	Removing Installation(s)	570
	Technical Support	570
	LearnKey Technical Support	570
Appendix B	OSI Model and Internet Protocols	571
	Networking Frameworks and Protocols	571
	OSI Model	572
	Application Layer	574
	Presentation Layer	575

Session Layer	575
Transport Layer	575
Network Layer	576
Data-Link Layer	576
Physical Layer	576
Internet Protocols	576
TCP	577
UDP	577
IP	577
Message Encapsulation	578
Review	579
Glossary	581
Index	601