

Contents

Introduction

xxiii

Chapter 1	Systems Security	1
1.1	Differentiate among various systems security threats.	3
	Privilege escalation	3
	Virus	4
	Worm	4
	Trojan	5
	Spyware	5
	Spam	5
	Adware	8
	Rootkits	8
	Botnets	9
	Logic bomb	10
	Exam Essentials	10
1.2	Explain the security risks pertaining to system hardware and peripherals.	11
	BIOS	11
	USB devices	12
	Cell phones	12
	Removable storage	13
	Network attached storage	14
	Exam Essentials	14
1.3	Implement OS hardening practices and procedures to achieve workstation and server security.	15
	Hotfixes	18
	Service packs	18
	Patches	18
	Patch management	19
	Group policies	19
	Security templates	20
	Configuration baselines	20
	Exam Essentials	21
1.4	Carry out the appropriate procedures to establish application security.	21
	ActiveX	22
	Java	22
	Scripting	23
	Browser	23
	Buffer overflows	24
	Cookies	24

	SMTP open relays	25
	Instant messaging	26
	P2P	27
	Input validation	27
	Cross-site scripting (XSS)	27
	Exam Essentials	28
1.5	Implement security applications.	29
	HIDS	29
	Personal software firewalls	29
	Antivirus	30
	Anti-spam	30
	Popup blockers	30
	Exam Essentials	30
1.6	Explain the purpose and application of virtualization technology.	31
	Exam Essentials	31
	Review Questions	32
	Answers to Review Questions	34
Chapter 2	Network Infrastructure	35
2.1	Differentiate between the different ports & protocols, their respective threats and mitigation techniques.	37
	Antiquated protocols	37
	TCP/IP hijacking	39
	Null sessions	40
	Spoofing	41
	Man-in-the-middle	41
	Replay	42
	DOS	43
	DDOS	46
	Domain Name Kiting	46
	DNS poisoning	47
	ARP poisoning	48
	Exam Essentials	49
2.2	Distinguish between network design elements and components.	50
	DMZ	51
	VLAN	53
	NAT	55
	Network interconnections	56
	NAC	58
	Subnetting	59
	Telephony	60
	Exam Essentials	61

2.3 Determine the appropriate use of network security tools to facilitate network security.	63
NIDS	63
NIPS	68
Firewalls	68
Proxy servers	70
Honeypot	71
Internet content filters	72
Protocol analyzers	72
Exam Essentials	73
2.4 Apply the appropriate network tools to facilitate network security.	73
NIDS	75
Firewalls	75
Proxy servers	75
Internet content filters	75
Protocol analyzers	75
Exam Essentials	75
2.5 Explain the vulnerabilities and mitigations associated with network devices.	76
Privilege escalation	76
Weak passwords	77
Back doors	78
Default accounts	79
DOS	80
Exam Essentials	80
2.6 Explain the vulnerabilities and mitigations associated with various transmission media.	80
Vampire taps	86
Exam Essentials	86
2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.	86
Data emanation	88
War driving	89
SSID broadcast	89
Blue jacking	89
Bluesnarfing	90
Rogue access points	90
Weak encryption	90
Exam Essentials	91
Review Questions	93
Answers to Review Questions	95

Chapter 3	Access Control	97
3.1	Identify and apply industry best practices for access control methods.	99
	Implicit deny	99
	Least privilege	100
	Separation of duties	100
	Job rotation	100
	Exam Essentials	100
3.2	Explain common access control models and the differences between each.	101
	Role & Rule Based Access Control	104
	Exam Essentials	104
3.3	Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.	105
	Exam Essentials	105
3.4	Apply appropriate security controls to file and print resources.	106
3.5	Compare and implement logical access control methods.	106
	ACL	106
	Group policies	106
	Password policy	107
	Domain password policy	107
	User names and passwords	107
	Time of day restrictions	108
	Account expiration	109
	Logical tokens	109
	Exam Essentials	110
3.6	Summarize the various authentication models and identify the components of each.	110
	One, two and three-factor authentication	111
	Single sign-on	112
	Exam Essentials	112
3.7	Deploy various authentication models and identify the components of each.	112
	Biometric reader	112
	RADIUS	113
	RAS	114
	LDAP	115
	Remote access policies	116
	Remote authentication	117
	VPN	117
	Kerberos	119

	CHAP	120
	PAP	122
	Mutual	122
	802.1x	122
	TACACS	122
	Exam Essentials	122
3.8	Explain the difference between identification and authentication (identity proofing).	123
	Exam Essentials	124
3.9	Explain and apply physical access security methods.	124
	Physical access logs/lists	125
	Hardware locks	126
	Physical access control – ID badges	126
	Door access systems	126
	Mantrap	127
	Physical tokens	127
	Video surveillance – camera types and positioning	128
	Exam Essentials	128
	Review Questions	129
	Answers to Review Questions	131
Chapter 4	Assessments and Audits	133
4.1	Conduct risk assessments and implement risk mitigation.	135
	Exam Essentials	136
4.2	Carry out vulnerability assessments using common tools.	137
	Port scanners	137
	Vulnerability scanners	138
	Protocol analyzers	138
	OVAL	138
	Password crackers	139
	Network mappers	140
	Exam Essentials	140
4.3	Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.	141
	Exam Essentials	141
4.4	Use monitoring tools on systems and networks and detect security-related anomalies.	142
	Performance monitor	142
	Systems monitor	142
	Performance baseline	142
	Protocol analyzers	143
	Exam Essentials	143

4.5 Compare and contrast various types of monitoring methodologies.	143
Behavior-based	143
Signature-based	144
Anomaly-based	144
Exam Essentials	144
4.6 Execute proper logging procedures and evaluate the results.	145
Security application	145
DNS	146
System	146
Performance	146
Access	146
Firewall	147
Antivirus	147
Exam Essentials	147
4.7 Conduct periodic audits of system security settings.	147
User access and rights review	148
Storage and retention policies	148
Group policies	148
Exam Essentials	149
Review Questions	150
Answers to Review Questions	152
Chapter 5	Cryptography
	153
5.1 Explain general cryptography concepts.	155
Key management	155
Steganography	157
Symmetric key	158
Asymmetric key	160
Confidentiality	161
Integrity and availability	161
Non-repudiation	162
Comparative strength of algorithms	163
Digital signatures	163
Whole disk encryption	164
Trusted Platform Module (TPM)	165
Single vs. Dual sided certificates	165
Use of proven technologies	165
Exam Essentials	165
5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.	168
SHA	169
MD5	169
LANMAN	170

NTLM	170
Exam Essentials	170
5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.	171
DES	171
3DES	171
RSA	171
PGP	171
Elliptic curve	172
AES	172
AES256	172
One time pad	173
Transmission encryption (WEP TKIP, etc)	173
Exam Essentials	173
5.4 Explain and implement protocols.	173
SSL/TLS	174
S/MIME	174
PPTP	175
HTTP vs. HTTPS vs. SHTTP	176
L2TP	177
IPSEC	177
SSH	178
Exam Essentials	179
5.5 Explain core concepts of public key cryptography.	180
Public Key Infrastructure (PKI)	181
Recovery agent	182
Public key	182
Private keys	183
Certificate Authority (CA)	183
Registration	184
Key escrow	185
Certificate Revocation List (CRL)	186
Trust models	188
Exam Essentials	189
5.6 Implement PKI and certificate management.	192
Public Key Infrastructure (PKI)	192
Recovery agent	192
Public key	192
Private keys	192
Certificate Authority (CA)	192
Registration	192
Key escrow	192
Certificate Revocation List (CRL)	192
Review Questions	193
Answers to Review Questions	195

Chapter 6	Organizational Security	197
6.1	Explain redundancy planning and its components.	199
	Hot site	199
	Cold site	200
	Warm site	200
	Backup generator	200
	Single point of failure	200
	RAID	201
	Spare parts	201
	Redundant servers	202
	Redundant ISP	202
	UPS	202
	Redundant connections	203
	Exam Essentials	203
6.2	Implement disaster recovery procedures.	203
	Planning	203
	Disaster recovery exercises	204
	Backup techniques and practices – storage	205
	Schemes	205
	Restoration	206
	Exam Essentials	206
6.3	Differentiate between and execute appropriate incident response procedures.	207
	Forensics	208
	Chain of custody	208
	First responders	209
	Damage and loss control	209
	Reporting – disclosure of	209
	Exam Essentials	210
6.4	Identify and explain applicable legislation and organizational policies.	210
	Secure disposal of computers	211
	Acceptable use policies	211
	Password complexity	211
	Change management	212
	Classification of information	212
	Mandatory vacations	213
	Personally Identifiable Information (PII)	213
	Due care	213
	Due diligence	213
	Due process	213
	SLA	214
	Security-related HR policy	214
	User education and awareness training	214
	Exam Essentials	215

6.5 Explain the importance of environmental controls.	217
Fire suppression	217
HVAC	218
Shielding	218
Exam Essentials	218
6.6 Explain the concept of and how to reduce the risks of social engineering.	218
Phishing	220
Hoaxes	220
Shoulder surfing	220
Dumpster diving	220
User education and awareness training	220
Exam Essentials	221
Review Questions	222
Answers to Review Questions	224
Appendix A	About the Companion CD
	225
<i>Index</i>	229