

TABLE OF CONTENTS

Acknowledgement	iv
About the Authors	v
Preface	vii
1. Cyber Security	1
Introduction	1
ICT Expansion	2
Need for Cyber Security	4
Consequences of Weak Security	6
Reasons for Cyber Crime	7
Cyber Criminals	8
List of Top 20 Countries with the Highest Rate of Cyber Crime	8
Defense Against Cyber-Crime	9
2. Desktop Security	11
Introduction	11
Why MAC Address is more reliable?	12
Tool for Checking MAC and IP	13
Types of Security Software	14
Implementing Power-on Password in a Computer System	15
Setting a Window Password	17
File Systems of Window Operating System	18
FAT File System	18
NTFS	18
Install the Latest Patches	27
Windows User Account	28
Set a Strong Password	28
Change Account Type	29
Disable Guest Account	31
Secure/Delete Unwanted User Accounts	31
Local Security Policies	32
Audit Policy	32
User Right Policy	33
Security Policy	36
Create a Password Policy and an Account Lockout Policy	37
Windows Event Logs	39
Turn off Simple File Sharing	39
System Protection	40
File Deletion from Recycle Bin	41
Install Anti-virus software	42
Select Tools	42
Using Microsoft Baseline Security Analyser(MBSA)	43
PC Audit	45
Secunia Personal Software Inspector (PSI)	45
Trend Micro Hijack	47
3. Operating System Security	55
Introduction	55
Role of Operating System	56
Windows Vulnerabilities	56
Password Vulnerabilities	57
Organizational password vulnerabilities:	57
Technical password vulnerabilities	57

x Table of Contents

Strong Passwords.....	58
Setting a Window Password:.....	58
Hardening Window OS.....	58
Setting the Basic Security Features.....	58
Setting the Intermediate Features.....	63
Windows Safe Mode.....	73
Select Tools.....	73
Ports.....	74
Listing Open Connections.....	74
Some Important ports.....	76
Select Port Scanning Tools.....	78
4. Network Vulnerabilities.....	81
Introduction.....	81
Network Architecture.....	83
OSI Architecture.....	83
TCP/IP Model.....	84
Need for Network Security.....	87
Select LAN Security Tools.....	87
Look@LAN:.....	88
NetworkView.....	94
Internet.....	96
World Wide Web.....	98
WHOIS.....	98
Regional Internet Registries(RIRs).....	99
Internet Protocol (IP).....	99
Types of IP Addresses.....	100
Internet Browser Security.....	103
Email Attacks.....	116
Email Set-up.....	116
Different Types of Email Client Exploits.....	117
E-mail surveillance.....	118
Email Protection.....	120
Spoofing("The False Digital Identity").....	121
Types of Spoofing.....	121
Some Network Vulnerability Scanners.....	122
Nessus.....	123
Nmap.....	134
5. Malicious Codes.....	143
Introduction.....	143
Computer Virus.....	143
Computer Virus Characteristics.....	144
Types of Viruses.....	144
Symptoms of a Computer Virus.....	145
Ways to trace a Computer Virus.....	145
Few Free Online Antivirus Tools.....	146
Malware.....	146
Spyware.....	147
Adware.....	147
Worms.....	148
Trojans.....	148
How Trojans Work?.....	149
Infection methods.....	149
Trojan Ports.....	151
Trojan Startup Methods.....	151
Integrated Development Environment.....	151

Key Loggers	151
Purpose of Key Logging	152
Select Tools	153
Precautionary Steps	154
6. Cryptography and Public Key Infrastructure.....	155
Introduction	155
Cryptography.....	156
Hashing Algorithms	157
Symmetric Algorithms	158
Asymmetric Key Encryption/Public Key Encryption.....	160
Encryption Strength and Key Length.....	162
Combining Symmetric Key and Public Key Encryption.....	162
Digital Signature Certificate(DSC)	163
Public Key Infrastructure Tool.....	165
7. Hacker Exploits and Countermeasures.....	181
Introduction	181
Stages of Hacking	182
Terminologies used in Hacking	183
What do Ethical Hackers do?.....	184
Types of Network Attacks.....	184
Spoofing(Identity spoofing or IP Address Spoofing).....	185
Sniffing.....	185
Mapping (Eavesdropping).....	186
Hijacking(Man-In-the-Middle Attack).....	186
Trojans	187
Denial-of-Service attack (DoS) and Distributed-Denial-of Service (DDoS) attacks.....	187
Social Engineering.....	190
Web and Network Security	190
SSL(Secured Socket Layer).....	190
IP Sec(IP Security)	191
Virtual Private Network.....	191
Firewalls.....	191
Few Tools	193
Security Related Websites.....	194
8. Cyber Crimes.....	195
Introduction	195
Types of Cyber Crimes.....	195
Financial Crimes	196
Cyber Pornography.....	196
Sale of illegal articles.....	196
Online Gambling.....	196
Intellectual Property crimes	196
Email spoofing	196
Forgery	197
Cyber Defamation.....	197
Cyber Stalking.....	197
Cybersquatting.....	197
E-Mail Bombing	197
Data Diddling	197
Salami Attack	197
Logic Bomb	197
Denial of Service	198
Virus and Worm	198
Trojan Horse.....	198
Motive Behind Cyber Crimes	198

xii Table of Contents

Social factors	198
Political agenda	198
Sexual impulses	198
Psychiatric Illness	199
Select Cases of Cyber Crimes.....	199
Select Cases of Cyber Crimes in Asia Pacific.....	200
Select Cases of Cyber Crimes In India.....	201
First Cases of Cyber Stalking in India	201
Pune Citibank Mphasis Call Center Fraud	202
Baazee.com case.....	202
State of Tamil Nadu Vs Suhas Katti Case	202
Domain Name Dispute: Yahoo Inc vs Akash Arora.....	204
Recent Cyber Crime Activities.....	204
9. Information System Audit.....	205
Introduction	205
Internal Audit	206
Professional Standards for Internal Audit	206
External Audit.....	206
Professional Standards for External Audit.....	206
Information System Audit.....	206
Information System Audit and Control Association.....	207
Need for Information System Auditors.....	207
Objectives of Information System Audit.....	208
IS Audit Vs Conventional Audit.....	208
Internal Control	208
Evidence Collection	209
Information System Control Objectives	210
Indian Standards in Auditing.....	210
Phases of Information System Audit.....	210
The Audit Charter.....	210
Review of Back Ground Material	210
IS Audit Plan	211
Risk and Vulnerability Assessment	211
Collection of Evidence	211
Evaluation of Evidence.....	212
Audit Report	212
Follow up of Audit Recommendations.....	212
Walk Through the Information System (Check-List)	212
Glossary.....	217
Appendix.....	221