

Contents

1	Cybersecurity for Beginners	1
1.1	Introduction to Cybersecurity	1
1.2	Necessity of Cybersecurity	2
1.3	Cybersecurity Challenges	2
1.4	Cybersecurity Threats	5
1.5	Cyberattack Life Cycle	5
1.6	Cybersecurity Principles	6
1.7	Cybersecurity Standards	7
1.8	Cybersecurity Framework	8
1.9	Fundamentals of Cybersecurity	9
1.10	Why is Cybersecurity Important?	9
1.10.1	Confidentiality	10
1.10.2	Integrity	11
1.10.3	Availability	11
1.11	Why Do We Implement Cybersecurity?	11
1.12	Cybersecurity Attacks and Their Types	12
1.12.1	Malware Attack	13
1.12.2	Phishing Attacks	14
1.12.3	Denial-of-Service Attacks	14
1.12.4	SQL Injection Attacks	16
1.12.5	Cross-Site Scripting	16
1.12.6	Man-In-The-Middle Attacks	17
1.13	Cybersecurity Development	18
1.14	Advantages of Cyber Security	18
1.15	Applications of Cybersecurity	19
2	The Basics of Hacking and Penetration Testing	21
2.1	Hacking Introduction	21
2.2	Ethical Hacking	22
2.3	Types of Cybercrime	24
2.4	Denial-of-Service Attacks (DoS)	27

2.5	Penetration Testing	31
2.5.1	Penetration Testing Versus Vulnerability Assessment	34
2.5.2	Types of Penetration Testing	34
2.5.3	Penetration Testing—Manual and Automated	36
2.5.4	Penetration Testing Tools	38
2.5.5	Infrastructure Penetration Testing	38
2.5.6	Penetration Testing—Tester	41
2.5.7	Penetration Testing—Report Writing	42
2.5.8	Penetration Testing—Ethical Hacking	44
2.5.9	Penetration Testing Limitations	45
3	Hacking for Dummies	47
3.1	Security Hacker	47
3.2	Classifications of Hacker	47
3.3	Common Hacking Tools	49
3.4	Common Hacking Techniques	49
3.4.1	Ethical Hacking	51
3.5	Developing Ethical Hacking Plan	54
3.6	Types of Security Testing	54
3.7	Ethical Hacking Tools	57
3.8	Physical Security	58
3.9	Risk Assessment	59
4	Networking All-In-One for Dummies	63
4.1	Network Introduction	63
4.2	Packet Network	63
4.3	Topology of Network	64
4.3.1	Types of Topologies	64
4.4	Operating System for the Network	69
4.5	Hardware Networking	73
4.5.1	Range of the Network Hardware	73
4.5.2	Computer Components of the Necessary Hardware	73
4.6	Network Setup	74
4.7	The Function of Prediction	76
4.8	Network Security	77
4.9	Defense Against Computers	78
4.10	Sharing of the Network	78
4.10.1	Operation of Network Sharing	79
4.11	Goals and Competences	81
4.11.1	Appearances of Problem-Solving	82

5	Effective Cybersecurity	87
5.1	Attacks and Vulnerabilities	87
5.2	Community of Security of Information	87
5.3	Cybersecurity Managed	88
5.4	Network Security Governance Framework	90
5.5	Risk Assessment of Structures	91
5.6	Security Evaluation Aim	92
5.6.1	Methodological Approach	92
5.6.2	Checking for Protection	93
5.6.3	Protection and Privacy	93
5.7	Evaluation of Risk	94
5.8	Study of the Cyber Danger	95
5.9	Risk Evaluation Forms	97
5.10	Safety for Software Development	98
5.11	Strike Cyber	99
5.12	Facts	99
6	Malware	103
6.1	What Does Malware Do?	103
6.2	How to Protect Against Malware?	104
6.3	Malware Analyzing Tools	105
6.3.1	Basic Malware Exploring Tools	105
6.3.2	Dynamic Malware Analyzing Tools	107
6.3.3	Difference Between Static and Dynamic Malware Analysis Tools	110
6.3.4	Warning Signs to Identify Malware Infection	111
6.4	Most Dangerous Malware of 2018	112
6.4.1	Malware Detection Techniques Used by Antivirus	112
6.4.2	Tips to Prevents the System from Malware Actions	114
7	Firewalls	117
7.1	Importance of Firewalls	117
7.2	Uses of Firewalls	118
7.3	How Does Firewall Works	118
7.4	Types of Firewall	119
7.5	Benefits of Firewalls	124
7.6	Advantages and Disadvantages of Firewalls	125
7.7	Firewall Threats and Vulnerability	125
8	Cryptography	129
8.1	Evaluation of Cryptography	129
8.2	Features of Cryptography	130
8.3	Types of Cryptography	131
8.4	Cryptography and Network Security Principles	132
8.5	Cryptographic Algorithms	133
8.6	Tools for Cryptography	135

8.7	Advantages and Disadvantages of Cryptography	137
8.8	Applications of Cryptography	138
9	Control Physical and Logical Access to Assets	141
9.1	Managing Access to Assets	141
9.2	Why Access Control is Required: The CIA Triad	142
9.3	Classification of Access Control	143
9.3.1	Preventive Access Control	144
9.3.2	Detective Access Control	144
9.3.3	Corrective Access Control	144
9.3.4	Deterrent Access Control	144
9.3.5	Recovery Access Control	145
9.3.6	Directive Access Control	145
9.3.7	Compensation Access Control	145
9.3.8	Administrative Access Controls	146
9.3.9	Logical/Technical Controls	146
9.3.10	Physical Access Controls	146
10	Manage the Identification and Authentication of People, Devices, and Services	149
10.1	Registration and Identity Proofing	150
10.2	Authorization and Accountability	150
10.3	Effective Password Mechanisms	152
11	Integrate Identity as a Third-Party Service	159
11.1	Identity Management Techniques	159
11.2	Credential Management Systems	164
12	Implement and Manage Authorization Mechanisms	167
13	Managing the Identity and Access Provisioning Life Cycle	173
14	Conduct Security Control Testing	181
15	Collect Security Process Data	193
16	Recovery Strategies for Database	201
17	Analyze Test Output and Generate a Report	209
18	Ensure Appropriate Asset Retention	215
19	Determine Information and Security Controls	223
	References	231