UNIT - I

Chapter 1 : Information Security Overview 1-1 to 1-61

✓ **Syllabus Topic :** The Importance of Information Protection 1-4

1.1 Information Security Overview 1-4

1.1.1 The Importance of Information Protection 1-4

✓ **Syllabus Topic :** The Evolution of Information Security 1-5

1.1.2 The Evolution of Information Security 1-5

✓ **Syllabus Topic :** Justifying Security Investment 1-6

1.1.3 Justifying Security Investment 1-6

✓ **Syllabus Topic :** Security Methodology 1-9

1.1.4 Security Methodology 1-9

✓ **Syllabus Topic :** How to Build a Security Program ? 1-12

1.1.5 How to Build a Security Program ? 1-12

✓ **Syllabus Topic :** The Impossible Job 1-16

1.1.6 The Impossible Job 1-16

✓ **Syllabus Topic :** The Weakest Link 1-17

1.1.7 The Weakest Link 1-17

✓ **Syllabus Topic :** Strategy and Tactics 1-18

1.1.8 Strategy and Tactics 1-18

✓ **Syllabus Topic :** Business Processes vs. Technical Controls 1-20

1.1.9 Business Processes vs. Technical Controls 1-20

1.2 Introduction to Risk 1-21

✓ **Syllabus Topic :** Threat Definition 1-22

1.2.1 Threat Definition 1-22

1.2.1.1 Threat Vectors 1-22

1.2.1.2 Threat Sources and Targets 1-23

✓ **Syllabus Topic :** Types of Attacks 1-24

1.2.2 Types of Attacks 1-24

1.2.2.1 Malicious Mobile Code 1-25

1.2.2.2 Malicious HTML 1-29

1.2.2.3 Advanced Persistent Threats (APTs) 1-30

1.2.2.4 Physical and Network-Layer Attacks 1-31

1.2.2.5 Application-Layer Attacks 1-33

1.2.2.6 Man-in-the-Middle (MITM) Attacks 1-34

E-next
THE NEXT LEVEL OF EDUCATION

https://E-next.in

Scanned by CamScanner

1.2.2.7 Wireless Attacks 1-37

✓ **Syllabus Topic :** Risk Analysis 1-38

1.2.3 Risk Analysis 1-38

✓ **Syllabus Topic :** Secure Design Principles 1-40

1.3 Secure Design Principle 1-40

✓ **Syllabus Topic :** The CIA Triad and Other Models 1-40

1.3.1 The CIA Triad and Other Models 1-40

✓ **Syllabus Topic :** Defense Models 1-43

1.3.2 Defense Models 1-43

✓ **Syllabus Topic :** Zones of Trust 1-45

1.3.3 Zones of Trust 1-45

✓ **Syllabus Topic :** Best Practices for Network Defense 1-47

1.3.4 Best Practices for Network Defense 1-47

1.3.4.1 Secure the Physical Environment 1-48

1.3.4.2 Keeping Patches Updated 1-48

1.3.4.3 Using an Antivirus Scanner (with Real-Time Scanning) 1-49

1.3.4.4 Use Firewall Software 1-49

1.3.4.5 Secure Network Share Permissions 1-49

1.3.4.6 Use Encryption 1-50

1.3.4.7 Securing Applications and their Configuration 1-50

1.3.4.8 Blocking Dangerous File Types 1-51

1.3.4.9 Secure P2P Services 1-54

1.3.4.10 Make Sure Programmers Program Securely 1-55

1.3.4.11 Back Up the System 1-55

1.3.4.12 Implement ARP Poisoning Defenses 1-56

1.4 Exam Pack (Review Questions) 1-60

- **Chapter Ends** 1-61

UNIT - II

➢ Chapter 2 : Authentication 2-1 to 2-40

✓ **Syllabus Topic :** Authentication 2-1

2.1 Authentication 2-1

2.1.1 Types of Authentication Methods 2-2

2.1.2 User Authentication Vs. Machine Authentication 2-4

2.1.3 Additional Uses for Authentication 2-4

2.1.3.1 SSH 2-4

2.1.3.2 IPSec 2-5

✓ **Syllabus Topic :** Authorization 2-5

2.2 Authorization 2-5

✓ Syllabus Topic : Encryption 2-6

2.3 Encryption 2-6

✓ **Syllabus Topic :** A Brief History of Encryption 2-6

2.3.1 A Brief History of Encryption 2-6

2.3.2 Cryptography 2-7

2.3.2.1 Cryptography Techniques 2-7

✓ **Syllabus Topic :** Symmetric-Key Cryptography 2-8

2.3.2.2 Symmetric-Key Encryption(Cryptography) 2-8

✓ **Syllabus Topic :** Public Key Cryptography 2-9

2.3.2.3 Public Key Cryptography 2-9

✓ **Syllabus Topic :** Public Key Infrastructure 2-10

2.3.2.4 Public Key Infrastructure 2-10

✓ **Syllabus Topic :** Storage Security : Storage Security Evolution 2-11

2.4 Storage Security 2-11

2.4.1 Evolution of Storage Security 2-11

✓ **Syllabus Topic :** Modern Storage Security 2-13

2.4.2 Modern Storage Security 2-13

✓ **Syllabus Topic :** Risk Remediation 2-14

2.4.3 Risk Remediation 2-14

2.4.3.1 Confidentiality Risks 2-14

2.4.3.2 Integrity Risks 2-20

2.4.3.3 Availability Risks 2-21

✓ **Syllabus Topic : Best Practices** 2-24

2.4.4 Best Practices 2-24

2.4.4.1 Zoning 2-25

2.4.4.2 Arrays 2-25

2.4.4.3 Servers 2-25

2.4.4.4 Staff 2-26

2.4.4.5 Offsite Data Storage 2-26

✓ **Syllabus Topic :** General Database Security Concepts, Understanding Database Security Layers 2-26

2.5 Database Security Concepts 2-26

2.5.1 Database Security Layers 2-26

https://E-next.in

Scanned by CamScanner

2.5.1.1 Server-Level Security 2-27
2.5.1.2 Network-Level Security 2-27
2.5.1.3 Data Encryption 2-28
2.5.1.4 Operating System Security 2-28
2.5.1.5 Managing Database Logins 2-28
✓ **Syllabus Topic :** Understanding Database-Level Security 2-29
2.5.2 Understanding Database-Level Security 2-29
2.5.2.1 Database Administration Security 2-29
2.5.2.2 Database Roles and Permissions 2-30
2.5.2.3 Object-Level Security 2-31
✓ **Syllabus Topic :** Using Application Security 2-32
2.5.3 Using Application Security 2-32
2.5.3.1 Limitations of Application-Level Security 2-33
✓ **Syllabus Topic :** Database Backup and Recovery 2-34
2.5.4 Database Backup and Recovery 2-34
2.5.4.1 Determining Backup Constraints 2-34
2.5.4.2 Determining Recovery Requirements 2-34
2.5.4.3 Types of Database Backups 2-35
✓ **Syllabus Topic :** Database Auditing and Monitoring 2-37
2.5.5 Database Auditing and Monitoring 2-37
2.5.5.1 Reviewing Audit Logs 2-38
2.5.5.2 Database Monitoring 2-38
2.6 Exam Pack (Review Questions) 2-39
- **Chapter Ends...** 2-40

UNIT - III

Chapter 3 : Secure Network Design 3-1 to 3-68
✓ **Syllabus Topic :** Secure Network Design 3-1
3.1 Secure Network Design 3-1
✓ **Syllabus Topic :** Introduction to Secure Network Design 3-2
3.1.1 Introduction to Secure Network Design 3-2
3.1.1.1 Acceptable Risk 3-3
✓ **Syllabus Topic :** Performance 3-5
3.1.2 Performance 3-5
✓ **Syllabus Topic :** Availability 3-8
3.1.3 Availability 3-8

✓ **Syllabus Topic :** Security 3-9
3.1.4 Security 3-9
3.1.4.1 Wireless Impact on the Perimeter 3-10
3.1.4.2 Remote Access Considerations 3-11
3.1.4.3 Internal Security Practices 3-13
3.1.4.4 Intranets, Extranets and DMZs 3-14
3.1.4.5 Outbound Filtering 3-16
✓ **Syllabus Topic :** Network Device Security 3-16
3.2 Network Device Security 3-16
✓ **Syllabus Topic :** Switch and Router Basics 3-16
3.2.1 Switch and Router Basics 3-16
3.2.1.2 TCP/IP 3-18
3.2.1.3 Hubs 3-23
3.2.1.4 Switches 3-24
3.2.1.5 Routers 3-25
✓ **Syllabus Topic :** Network Hardening 3-27
3.2.2 Network Hardening 3-27
3.2.2.1 Patching 3-28
3.2.2.2 Switch Security Practices 3-28
3.2.2.3 Access Control Lists 3-29
3.2.2.4 Disabling Unused Services 3-30
3.2.2.5 Administrative Practices 3-32
3.2.2.6 Internet Control Message Protocol (ICMP) 3-36
3.2.2.7 Anti-Spoofing and Source Routing 3-39
3.2.2.8 Logging 3-40
3.3 Firewalls 3-40
✓ **Syllabus Topic :** Overview 3-40
3.3.1 Overview of Firewalls 3-40
✓ **Syllabus Topic :** The Evolution of Firewalls 3-41
3.3.1.1 The Evolution of Firewalls 3-41
3.3.1.2 Application Control 3-42
3.3.1.3 Must-Have Firewall Features 3-43
✓ **Syllabus Topic :** Core Firewall Functions 3-44
3.3.2 Core Firewall Functions 3-44
3.3.2.1 Network Address Translation (NAT) 3-45
3.3.2.2 Auditing and Logging 3-48

E-next
THE NEXT LEVEL OF EDUCATION

Scanned by CamScanner

✓ **Syllabus Topic :** Additional Firewall Capabilities 3-48
3.3.3 Additional Firewall Capabilities 3-48
3.3.3.1 Application and Website Malware Execution Blocking 3-48
3.3.3.2 Antivirus 3-49
3.3.3.3 Intrusion Detection and Intrusion Prevention 3-49
3.3.3.4 Web Content (URL) Filtering and Caching 3-49
3.3.3.5 E-Mail (Spam) Filtering 3-49
3.3.3.6 Enhance Network Performance 3-50
✓ **Syllabus Topic :** Firewall Design 3-50
3.3.4 Firewall Design 3-50
3.3.4.1 Firewall Strengths and Weaknesses 3-51
3.3.4.2 Firewall Placement 3-51
3.3.4.3 Firewall Configuration 3-52
✓ **Syllabus Topics :** Radio Frequency Security Basics 3-52
3.4 Radio Frequency Security 3-52
3.5 Data-Link Layer 3-52
✓ **Syllabus Topics :** Data- Link Layer Wireless Security Features 3-53
3.5.1 Data-Link Layer Features 3-53
✓ **Syllabus Topics :** Data- Link Layer Wireless Security Flaws 3-54
3.5.2 Data-Link Layer Flaws 3-54
✓ **Syllabus Topics :** Threats 3-55
3.5.3 Network Security : Common Threats 3-55
✓ **Syllabus Topics :** Mitigation 3-57
3.5.4 Mitigation Techniques 3-57
3.5.6 WLAN security 3-58
✓ **Syllabus Topics :** Wireless Vulnerabilities 3-59
3.5.7 Threats and Vulnerabilities 3-59
3.5.7.1 Steps to Securing Wireless Networks 3-60
3.5.7.2 Taking Stock 3-60
✓ **Syllabus Topics :** Wireless Network Hardening Practices and Recommendations 3-61
3.6 Hardening 3-61
✓ **Syllabus Topics :** Wireless Intrusion Detection and Prevention 3-65
3.7 Wireless Intrusion Detection and Prevention System 3-65
3.7.1 WIDS (Wireless Intrusion Detection System) 3-65
3.7.2 WIPS (Wireless Intrusion Prevention System) 3-65
3.8 Exam Pack (Review Questions) 3-67
- **Chapter Ends** 3-67

UNIT - IV

➤ **Chapter 4 : Intrusion Detection System** 4-1 to 4-49
✓ **Syllabus Topic :** Intrusion Detection System : Concepts, Detection Models, IDS Features 4-1
4.1 Intrusion Detection Systems 4-1
4.1.1 Intrusion Detection Tools 4-1
✓ **Syllabus Topic :** IDS Types 4-2
4.1.2 Types of IDS 4-2
4.2 Passive and Reactive Systems 4-3
✓ **Syllabus Topic :** Intrusion Prevention Systems 4-3
4.2.1 Intrusion Prevention Systems 4-3
4.2.2 Detection Methods 4-4
✓ **Syllabus Topic :** IDS Deployment Consideration 4-5
4.2.3 IDS Deployment Consideration 4-5
4.2.4 Comparing IPS versus IDS 4-6
4.2.5 Gaining IDS Mindshare 4-7
4.2.6 Gather Network Topology Diagrams 4-8
4.2.7 Identify Physical Infrastructure 4-8
4.2.8 Sensor Topology Discussion 4-8
4.2.9 Pre- Installation Phase 4-10
✓ **Syllabus Topic :** Security Information and Event Management (SIEM) 4-11
4.3 Security Information and Event Management (SIEM) 4-11
✓ **Syllabus Topic :** Voice Over IP (VOIP) : Background 4-13
4.4 VOIP 4-13
✓ **Syllabus Topic :** VoIP Components 4-14
4.4.1 VoIP Components 4-14
✓ **Syllabus Topic :** VOIP Vulnerabilities and Countermeasures 4-17
4.4.2 VOIP Vulnerabilities and Countermeasures 4-17
✓ **Syllabus Topic :** PBX Security 4-21
4.5 Private Branch Exchange (PBX) 4-21
✓ **Syllabus Topic :** TEM : Telecom Expense Management 4-21
4.6 Telecom Expense Management (TEM) 4-21
✓ **Syllabus Topic :** Operating System Security Models : Classic Security Models 4-23
4.7 Security Models 4-23
4.7.1 Introduction 4-23

E-next
THE NEXT LEVEL OF EDUCATION

https://E-next.in

Scanned by CamScanner

4.7.2 Computer Security Classifications 4-25
✓ **Syllabus Topic :** Operating System Models....................4-30
4.7.3 Operating System Models 4-30
✓ **Syllabus Topic :** Reference Monitor....................4-30
4.7.4 Reference Monitor....................4-30
✓ **Syllabus Topic :** Trustworthy Computing....................4-31
4.7.5 Trustworthy Computing 4-31
4.8 Common Attack Vectors 4-32
4.9 Hosting, Hardware, Firmware and Other Invisible Threats 4-35
4.9.1 Security Personas 4-36
4.9.2 Benefits of Personas 4-36
4.10 Threat Models....................4-38
4.10.1 Privacy Management Reference Model 4-39
4.10.2 NIST Security Framework 4-40
4.10.3 Jericho Security Model....................4-40
4.11 Security Architecture Landscape....................4-41
4.12 Software Assurance Maturity Model (SAMM)....................4-42
4.13 Security within the SDLC process 4-43
4.14 IoT Threat Model 4-43
4.15 NIST Cloud Computing Security Model....................4-45
4.16 Mobile Threat Model....................4-45
4.17 DDoS Model....................4-45
✓ **Syllabus Topic :** International Standards for Operating System Security 4-46
4.18 International Standards for Operating System Security....................4-46
4.19 Exam Pack (Review Questions)....................4-47
- **Chapter Ends**....................4-49

UNIT - V

➢ Chapter 5 : Virtual Machines and Cloud Computing 5-1 to 5-56

✓ **Syllabus Topic :** Virtual Machines....................5-1
5.1 Virtual Machines 5-1
✓ **Syllabus Topic :** Cloud Computing....................5-3
5.2 Cloud Computing 5-3
5.2.1 Software as a Service (SaaS)....................5-3
5.2.2 Platform as a Service (PaaS) 5-4
5.2.3 Infrastructure as a Service (IaaS) 5-4

5.2.4 Comparison between IaaS, PaaS and SaaS 5-4
✓ **Syllabus Topic :** Secure Development Lifecycle....................5-5
5.3 Secure Development Lifecycle 5-5
5.3.1 Defining the Secure Development Lifecycle 5-6
5.3.2 The Problems the SDL Solves....................5-6
5.3.3 People, Process and Technology....................5-7
5.3.4 SDL Phases....................5-7
5.3.4.1 The Requirements Phase 5-8
5.3.4.2 The Design Phase 5-8
5.3.4.3 Implementation or Coding....................5-9
5.3.4.4 The Test Phase....................5-9
5.3.4.5 The Final Phase : Release/Response 5-10
✓ **Syllabus Topic :** Application Security Practices....................5-10
5.4 Application Security Practices 5-10
5.4.1 Recommendations for App-Focused Security....................5-11
✓ **Syllabus Topic :** Web Application Security....................5-14
5.5 Web Application Security Best Practices....................5-14
✓ **Syllabus Topic :** Client Application Security 5-21
5.6 Client Application Security 5-21
5.6.1 Thick Client Vs Thin Client Applications....................5-21
5.6.2 Security Assessment of Thick Client Applications....................5-22
5.6.3 List of Tools that can used Intercepting Thick Client Applications 5-23
5.6.4 Critical Vulnerabilities Faced by Thick Client Application....................5-26
5.6.4.1 Sensitive Data Storage on Files and Registries....................5-26
5.6.4.2 Process Monitor....................5-26
5.6.4.3 Registry Monitoring 5-26
5.6.4.4 File Monitoring....................5-27
✓ **Syllabus Topic :** Remote Administration Security 5-27
5.7 Securing Remote Desktop (RDP) for System Administrators 5-27
5.7.1 Basic Security Tips for Remote Desktop 5-27
5.7.2 Limit Users Who Can Log in Using Remote Desktop 5-29
5.7.3 Set an Account Lockout Policy 5-29
5.8 Best Practices for Additional Security 5-30
✓ **Syllabus Topic :** Classification of Assets....................5-33
5.9 Classification of Assets 5-33

E-next THE NEXT LEVEL OF EDUCATION

Scanned by CamScanner

✓ **Syllabus Topic :** Physical Security, Physical Vulnerability Assessment 5-34
5.10 Physical Security 5-34
✓ **Syllabus Topic :** Choosing Site Location for Security 5-35
5.11 Choosing Site Location for Security 5-35
5.12 Assets and Security Requirements 5-38
5.12.1 Critical Assets 5-38
5.12.2 Security Requirements 5-39
✓ **Syllabus Topic :** Securing Assets 5-39
5.13 Securing Assets 5-39
5.13.1 ID Cards and Badges 5-40
5.13.2 Other Access Mechanisms 5-41
✓ **Syllabus Topic :** Locks and Entry Controls 5-42
5.13.3 Locks and Keys 5-42
5.13.4 Electronic Monitoring and Surveillance Cameras 5-42
5.13.5 Alarms and Alarm Systems 5-43
✓ **Syllabus Topic :** Physical Intrusion Detection 5-43
5.13.6 Biometrics 5-43
5.13.6.1 Some of the Important Biometric Mechanisms 5-44
5.13.6.2 Biometric Access System 5-47
5.13.6.3 Performance of the Biometrics System 5-48
5.13.6.4 The Test of a Good Biometric System 5-49
5.13.6.5 Multimodal Biometric System 5-50
5.14 Administrative Controls 5-51
5.14.1 Fire Safety Factors 5-51
5.15 Interception of Data 5-53
5.15.1 Mobile and Portable Devices 5-54
5.15.2 Visitor Control 5-55
5.16 Exam Pack (Review Questions) 5-55
- **Chapter Ends 5-56**
- **List of Practicals ..... L-1 to L76**
- **Model Question Papers ..... M-1 to M-4**

□□□

1.1.5
1.3.2
2.3.5
5.2.1
5.5.4

E-next
THE NEXT LEVEL OF EDUCATION

CHAPTER 1 Information Security Overview

Unit I

Introduction

Q. 1 Explain the term Security and hence explain Information Security. (Ref. Introduction) **(5 Marks)**

What is security?

In general, security is "the quality or state of being secure" which simply means "to be free from danger". In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. A successful organization should have the following multiple layers of security in place to protect its operations :

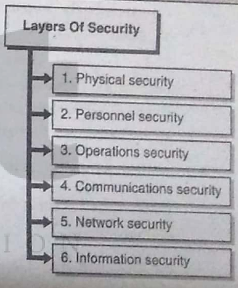

Fig. 1 : Layers of security

1. Physical security

To protect physical items, objects, or areas from unauthorized access and misuse.

2. Personnel security

To protect the individual or group of individuals who are authorized to access the organization and its operations.

3. Operations security

To protect the details of a particular operation or series of activities.

4. Communications security

To protect communications media, technology and content.

Scanned by CamScanner