

**Unit I****Chapter 1 : Introduction and Access Control****1-1 to 1-20****Syllabus :**

Cyber-attacks, Vulnerabilities, Defence Strategies and Techniques, Authentication Methods and Protocols, Defence in Depth Strategies. Access Control Policies: DAC, MAC, Multi-level Security Models: Biba Model, Bell La Padula Model, Single Sign on, Federated Identity Management.

1.1	Introduction.....	1-1
1.2	Cyber-Attacks.....	1-2
1.2.1	Types of Cyber Attacks	1-2
1.3	Vulnerabilities	1-3
1.4	Defence Strategies and Techniques	1-3
1.5	Authentication Methods	1-5
1.6	Authentication Protocols.....	1-7
1.6.1	One-Way Authentication Protocols.....	1-8
1.6.2	Mutual Authentication.....	1-9
1.7	Defence in Depth Strategies (DiD).....	1-11
1.8	Access Control Policies	1-12
1.8.1	Discretionary Access Control (DAC).....	1-12
1.8.2	Mandatory Access Control (MAC).....	1-14
1.8.3	Multi-Level Security Models	1-15
1.8.4	Bell La Padula Model.....	1-15
1.8.5	Biba Model	1-17
1.9	Single Sign on	1-17
1.10	Federated Identity Management	1-18
1.10.1	Security Assertion Markup Language (SAML)	1-19

Unit II**Chapter 2 : Program and OS Security****2-1 to 2-27****Syllabus :**

Malicious and Non-Malicious programming errors, Targeted Malicious codes: Salami Attack, Linearization Attack, Covert Channel, Control against Program threats.

Operating System Security: Memory and Address protection, File Protection Mechanism, User Authentication.

Linux and Windows: Vulnerabilities, File System Security.

2.1	Malicious and Non-Malicious Programming Errors	2-1
2.1.1	Types of Malicious Code	2-2
2.2	Targeted Malicious Code.....	2-3
2.2.1	Salami Attack	2-4
2.2.2	Linearization Attack	2-4
2.3	Non-Malicious Errors	2-5
2.3.1	Covert Channel.....	2-7
2.4	Control against Program Threats.....	2-8
2.5	Operating System Security	2-13
2.5.1	Protection in General Purpose OS.....	2-13
2.6	Memory and Address Protection.....	2-14
2.6.1	Approaches of Memory Protection.....	2-14
2.7	File Protection Mechanism	2-21
2.7.1	Different File Protection Methods.....	2-21
2.8	User Authentication	2-22
2.9	Linux and Windows Vulnerability	2-23
2.9.1	Windows Vulnerabilities.....	2-24
2.10	File System Security.....	2-24
2.10.1	Linux File System Security	2-25
2.10.2	Windows File System Security	2-26

Unit III**Chapter 3 : Web Application Security****3-1 to 3-31****Syllabus :**

OWASP, Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Click jacking, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, Web Service Security, OAuth 2.0

3.1	OWASP.....	3-1
3.2	Web Security Consideration	3-2
3.3	User Authentication and Session Management	3-3
3.4	Cookies	3-4



3.5	SSL and HTTPS.....	3-5	4.5.1	Security Threats	4-6
3.5.1	SSL Architecture	3-6	4.5.2	Device Security	4-7
3.6	SSH.....	3-10	4.6	GSM and UMTS Security	4-8
3.7	Privacy on Web	3-12	4.6.1	GSM	4-8
3.8	Web Browser Attacks	3-13	4.6.1(A)	Components	4-9
3.9	Account Harvesting	3-15	4.6.1(B)	Temporary Mobile Subscriber Identity	4-9
3.10	Web Bugs.....	3-16	4.6.1(C)	Cryptographic Algorithms	4-9
3.11	Clickjacking	3-16	4.6.1(D)	Subscriber Identity Authentication	4-10
3.12	Cross-Site Request Forgery	3-17	4.6.1(E)	Encryption	4-11
3.13	Session Hijacking and Management.....	3-18	4.6.1(F)	Location-Based Services	4-11
3.13.1	Session Management.....	3-18	4.6.2	UMTS	4-11
3.13.2	Session Hijacking	3-20	4.6.2(A)	False Base Station Attacks.....	4-11
3.14	Phishing and Pharming Techniques	3-21	4.6.2(B)	Cryptographic Algorithms	4-12
3.14.1	Pharming Techniques.....	3-22	4.6.2(C)	UMTS Authentication and Key Agreement	4-12
3.15	Web Service Security	3-23	4.7	IEEE 802.11/802.11i Wireless LAN Security	4-13
3.15.1	Web Services Security Architecture	3-24	4.7.1	IEEE 802.11	4-13
3.16	OAuth 2.0	3-29	4.7.1(A)	Architecture of IEEE 802 Protocols	4-14

Unit IV

Chapter 4 : Wireless Security 4-1 to 4-26

Syllabus :

Wi-Fi Security, WEP, WPA, WPA-2, Mobile Device Security - Security Threats, Device Security, GSM and UMTS Security, IEEE 802.11/802.11i Wireless LAN Security, VPN Security.

4.1	Wi-Fi Security.....	4-1	4.8	VPN Security.....	4-22
4.1.1	Wireless Network Threats	4-2	4.8.1	Tunnelling.....	4-23
4.1.2	Wireless Security Measures	4-2	4.8.2	VPN Tunneling Protocols	4-24
4.1.3	Securing Wireless Access Points	4-3	4.8.3	Encryption in VPN	4-25
4.1.4	Securing Wireless Networks.....	4-3	4.8.4	Authentication.....	4-25
4.2	WEP (Wireless Equivalent Privacy).....	4-3	4.8.5	Features of a Typical VPN.....	4-25
4.3	WPA (WiFi Protected Access).....	4-4	4.8.6	Benefits of VPN.....	4-26
4.4	WPA-2.....	4-5	4.8.7	Disadvantage of VPN	4-26
4.5	Mobile Device Security	4-6			

**Unit V****Chapter 5 : Legal and Ethical Issues 5-1 to 5-43****Syllabus :**

Cybercrime and its types, Intellectual property, Privacy, Ethical issues.

Protecting Programs and Data, Information and the Law, Rights of Employees and Employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security, Case studies of ethics.

5.1	Cybercrime and Its Types.....	5-1
5.1.1	Types of Cybercrime/ Categories of Cybercrimes.....	5-1
5.2	Intellectual Property.....	5-4
5.2.1	Types of Intellectual Property	5-4
5.2.2	Intellectual Property Issues and Computer Security	5-5
5.3	Privacy	5-9
5.3.1	EU Privacy Law	5-9
5.3.2	US Privacy Law	5-9
5.3.3	Organizational Response	5-10
5.4	Ethical Issues	5-11
5.5	Protecting Programs and Data	5-13
5.5.1	Guidelines for Using the Law to Protect Computer Objects	5-20
5.6	Information and the Law	5-20
5.6.1	Information as an Object	5-20
5.6.2	Legal Issues Relating to Information.....	5-22
5.6.3	Protecting Information	5-22
5.7	Rights of Employees and Employers	5-24
5.8	Redress for Software Failures	5-26
5.9	Computer Crime	5-30
5.9.1	Examples of Statutes.....	5-32
5.10	Ethical Issues in Computer Security	5-35
5.10.1	Examples of Ethical Principles.....	5-38
5.10.1(A)	Consequence-Based Principles	5-38

5.10.1(B)	Rule-Based Principles	5-38
5.11	Case Studies of Ethics	5-39

Unit VI**Chapter 6 : Digital Forensics 6-1 to 6-36****Syllabus :**

Introduction to Digital Forensics, Acquiring Volatile Data from Windows and Unix systems, Forensic Duplication Techniques, Analysis of forensic images using open source tools like Autopsy and SIFT, Investigating logs from Unix and windows systems, Investigating Windows Registry.

6.1	Introduction to Digital Forensics	6-1
6.1.1	Digital Forensic.....	6-1
6.1.2	Why is digital forensics important ?	6-1
6.1.3	Digital Forensic Process Steps.....	6-1
6.2	Evidence	6-3
6.2.1	Types of Evidences	6-3
6.2.2	Evidence Characteristics	6-4
6.2.3	Challenges in Evidence Handling	6-4
6.2.4	Ethical Issues	6-5
6.3	Introduction to Incident	6-5
6.3.1	Goals of Incident Response.....	6-6
6.4	Acquiring Volatile Data from Windows and Unix Systems	6-6
6.4.1	Initial Response and Volatile Data Collection from Windows System.....	6-6
6.4.1(A)	Creating a Response Toolkit	6-7
6.4.1(B)	Storing Information Obtained During the Initial Response.....	6-9
6.4.1(C)	Obtaining Volatile Data.....	6-10
6.4.2	Initial Response and Volatile Data Collection from UNIX System	6-13
6.4.2(A)	Creating a Response Toolkit	6-14
6.4.2(B)	Storing Information Obtained During the Initial Response.....	6-14



6.4.2(C) Obtaining Volatile Data Prior to Forensic Duplication.....	6-15	6.6 Analysis of Forensic Images Using Open Source Tools like Autopsy and SIFT.....	6-23
6.5 Forensic Duplication Techniques.....	6-18	6.6.1 Autopsy	6-23
6.5.1 Forensic Duplicates as Admissible	6-18	6.6.2 SIFT	6-24
6.5.1(A) Forensic Duplicate.....	6-18	6.6.3 The Evidence Analysis Techniques in Autopsy.....	6-28
6.5.1(B) Qualified Forensic Duplicate.....	6-19	6.6.4 Evidence Search Techniques	6-28
6.5.1(C) Restored Image.....	6-19	6.7 Investigating Logs from Unix and Windows Systems	6-29
6.5.1(D) Mirror Image	6-20	6.7.1 Windows System Logs	6-29
6.5.2 Forensic Duplication Tool Requirements	6-20	6.7.2 Unix System Logs	6-31
6.5.3 Creating a Forensic Duplicate of Hard Drive.....	6-21	6.8 Investigating Windows Registry.....	6-33
6.5.4 Creating Qualified Forensic Duplicate of a Hard Drive.....	6-22	6.8.1 Windows Registry Organization.....	6-34