

**UNIT - I****Chapter 1 : Cybercrime and Ethical Hacking****1-1 to 1-24****Syllabus :**

Introduction to Cybercrime, Types of Cybercrime, Classification of Cybercriminals, Role of computer in Cybercrime, Prevention of Cybercrime.

Ethical Hacking, Goals of Ethical Hacking, Phases of Ethical Hacking, Difference between Hackers, Crackers and Phreakers, Rules of Ethical Hacking.

**Self Learning Topics :** Exploring various online hacking tools for Reconnaissance and scanning Phase.

<b>1.1</b>	<b>Introduction to Cybercrime.....</b>	<b>1-1</b>
1.1.1	Types of Cybercrime.....	1-2
1.1.2	Classification of Cybercriminals.....	1-5
<b>1.2</b>	<b>Role of Computer in Cybercrime .....</b>	<b>1-6</b>
<b>1.3</b>	<b>Prevention of Cybercrime .....</b>	<b>1-7</b>
<b>1.4</b>	<b>Ethical Hacking .....</b>	<b>1-9</b>
1.4.1	Goals of Ethical Hacking.....	1-10
<b>1.5</b>	<b>Phases of Ethical Hacking.....</b>	<b>1-11</b>
<b>1.6</b>	<b>Difference between Hackers, Crackers and Phreakers.....</b>	<b>1-13</b>
<b>1.7</b>	<b>Rules of Ethical Hacking.....</b>	<b>1-16</b>
<b>1.8</b>	<b>Self Learning Topics : Exploring Various Online Hacking Tools for Reconnaissance and Scanning Phase .....</b>	<b>1-17</b>
1.8.1	Tools used for Reconnaissance .....	1-17
1.8.2	Tools used for Scanning Network Vulnerabilities.....	1-21

**UNIT II****Chapter 2 : Digital Forensics Fundamentals****2-1 to 2-34****Syllabus :**

Introduction to Digital Forensics, Need and Objectives of Digital Forensics, Types of Digital Forensics, Process of Digital Forensics, Benefits of Digital Forensics, Chain of Custody, Anti Forensics.

Digital Evidence and its Types, Rules of Digital Evidences.

Incident Response, Methodology of Incident Response, Roles of CSIRT in handling incident.

**Self Learning Topics :** Pre Incident preparation and Incident Response process.

<b>2.1</b>	<b>Introduction to Digital Forensics.....</b>	<b>2-1</b>
------------	---	------------

2.1.1	Need and Objectives of Digital Forensics .....	2-2
<b>2.2</b>	<b>Types of Digital Forensics .....</b>	<b>2-4</b>
<b>2.3</b>	<b>Process of Digital Forensics.....</b>	<b>2-6</b>
<b>2.4</b>	<b>Benefits of Digital Forensics.....</b>	<b>2-9</b>
<b>2.5</b>	<b>Chain of Custody.....</b>	<b>2-9</b>
<b>2.6</b>	<b>Anti Forensics.....</b>	<b>2-11</b>
2.6.1	Anti-Forensic Techniques .....	2-12
<b>2.7</b>	<b>Digital Evidence and its Types.....</b>	<b>2-14</b>
2.7.1	Rules of Digital Evidences.....	2-15
<b>2.8</b>	<b>Incident Response .....</b>	<b>2-16</b>
2.8.1	Computer Security Incident .....	2-16
2.8.2	Goals of Incident Response.....	2-17
2.8.3	Methodology of Incident Response .....	2-17
<b>2.9</b>	<b>Roles of CSIRT in Handling Incident.....</b>	<b>2-19</b>
2.9.1	The CSIRT Core Team.....	2-19
2.9.2	Technical Support Personnel.....	2-21
2.9.3	Organizational Support Personnel.....	2-23
<b>2.10</b>	<b>Self Learning Topics : Pre-Incident Preparation and Incident Response Process .....</b>	<b>2-25</b>

**UNIT III**

**Chapter 3 : Computer Forensics**

**3-1 to 3-61**

**Syllabus :**

Introduction to Computer Forensics, Evidence collection (Disk, Memory, Registry, Logs etc), Evidence Acquisition, Analysis and Examination (Window, Linux, Email, Web, Malware), Challenges in Computer Forensics, Tools used in Computer Forensics.

**Self Learning Topics :** Open source tool for Data collection & analysis in windows or Unix.

<b>3.1</b>	<b>Introduction to Computer Forensics.....</b>	<b>3-1</b>
3.1.1	Advantages of Computer Forensics.....	3-2
3.1.2	Disadvantages of Computer Forensics.....	3-2
<b>3.2</b>	<b>Evidence collection (Disk, Memory, Registry, Logs etc.) .....</b>	<b>3-2</b>
3.2.1	Disk.....	3-2

3.2.2	Memory .....	3-6
3.2.3	Registry .....	3-9
3.2.4	Logs .....	3-13
<b>3.3</b>	<b>Evidence Acquisition .....</b>	<b>3-15</b>
<b>3.4</b>	<b>Analysis and Examination (Window, Linux, Email, Web, Malware).....</b>	<b>3-20</b>
3.4.1	Investigating Live Systems Windows.....	3-20
3.4.2	Investigating Live Linux System .....	3-31
3.4.3	Email Analysis.....	3-39
3.4.4	Analysis of Web.....	3-44
3.4.4(A)	Cookie Storage and Analysis .....	3-46
3.4.4(B)	Analyzing Cache and Temporary Internet Files .....	3-47
3.4.5	Analysis of Malware.....	3-49
<b>3.5</b>	<b>Challenges in Computer Forensics .....</b>	<b>3-51</b>
3.5.1	Technical Challenges .....	3-51
3.5.2	Legal Challenges.....	3-52
3.5.3	Resource Challenges.....	3-52
<b>3.6</b>	<b>Tools used in Computer Forensics.....</b>	<b>3-53</b>
<b>3.7</b>	<b>Self Learning Topics : Open-Source Tool for Data Collection &amp; Analysis in Windows or Unix.....</b>	<b>3-59</b>

## UNIT -IV

### Chapter 4 : Network Forensics

4-1 to 4-33

#### Syllabus :

Introduction, Evidence Collection and Acquisition (Wired and Wireless), Analysis of network evidences (IDS, Router), Challenges in network forensics, Tools used in network forensics.

**Self Learning Topics :** IDS types and role of IDS in attack prevention.

<b>4.1</b>	<b>Network Forensics Introduction.....</b>	<b>4-1</b>
<b>4.2</b>	<b>Evidence Collection and Acquisition (Wired and Wireless) .....</b>	<b>4-3</b>
4.2.1	What is Network based Evidence?.....	4-3
4.2.2	What are the Goals of Network Monitoring? .....	4-4

4.2.3 Types of Network Monitoring..... 4-4

4.2.4 Setting up a Network Monitoring System ..... 4-5

4.2.5 Performing a Trap-and-Trace ..... 4-10

4.2.6 Using TCPDUMP for Full Content Monitoring..... 4-11

4.2.7 Collecting Network-based Log Files..... 4-11

**4.3 Analysis of Network Evidences (IDS, Router) ..... 4-12**

4.3.1 Obtaining Volatile Data Prior to Powering Down ..... 4-13

4.3.2 Finding the Proof..... 4-14

4.3.2(A) Direct Compromise..... 4-14

4.3.2(B) Handling Routing Table Manipulation Incidents ..... 4-17

4.3.2(C) Handling Theft of Information Incidents..... 4-17

4.3.2(D) Handling Denial-of-Service (DoS) Attacks ..... 4-17

4.3.3 Using Routers as Response Tools..... 4-19

**4.4 Challenges in Network Forensics ..... 4-21**

**4.5 Tools used in Network Forensics ..... 4-25**

**4.6 Self-Learning Topics : IDS Types and Role of IDS in Attack Prevention ..... 4-29**

4.6.1 Intrusion Detection System..... 4-29

4.6.1(A) Types of IDS..... 4-31

4.6.1(B) IDS Advantages and Disadvantages..... 4-32

4.6.2 Role of IDS in Attack Prevention..... 4-32

**UNIT V**

**Chapter 5 : Mobile Forensics 5-1 to 5-18**

**Syllabus :**  
 Introduction, Evidence Collection and Acquisition, Analysis of Evidences, Challenges in mobile forensics, Tools used in mobile forensics  
**Self Learning Topics :** Tools / Techniques used in mobile forensics.

**5.1 Introduction.....5-1**

5.1.1 Mobile Phone Basics ..... 5-2

5.1.2 Inside Mobile Devices ..... 5-5

**5.2 Evidence Collection and Acquisition .....5-6**  
     5.2.1 Evidence Acquisition ..... 5-10

**5.3 Analysis of Evidences ..... 5-12**

**5.4 Challenges in Mobile Forensics ..... 5-12**

**5.5 Tools used in Mobile Forensics ..... 5-15**

**5.6 Self-Learning Topics : Tools / Techniques used in Mobile Forensics..... 5-16**

**UNIT -VI**

**Chapter 6 : Report Generation**

**6-1 to 6-16**

**Syllabus :**

Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a forensic report.

**Self Learning Topics :** For an incident write a forensic report.

**6.1 Goals of Report .....6-1**

**6.2 Layout of an Investigative Report .....6-2**

**6.3 Guidelines for Writing a Report.....6-6**

**6.4 Sample for Writing a Forensic Report ..... 6-11**

**6.5 Self-Learning Topics : For an Incident Write a Forensic Report ..... 6-12**