BCA (Semester- 6)

Teaching Schedule

030010608: SEC1 Fundamentals of Cyber Security

Prior Topic Learning: Fundamentals of Computers, Internet and Network

Course Objective: To imbibe the fundamentals of cybersecurity and its legal perspectives as well as examine the need of cryptography and digital forensics for securing information in the cyber world.

Course Outcomes: Upon completion of the course, the student shall be able to
CO1: Recognize the cyber crime and its importance including the act of cyber criminals along with its types.
CO2: Classify passive and active types of cyber-attacks and prevent them by using different techniques such as strong password, protect identity online, protect computer with security software.
CO3: Classify and relate methods used in cybercrime along with common security mechanism.
CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
CO5: Identify the cyber laws against cyber crime, especially in the Indian context.
CO6: Investigate the importance of digital forensics with its phases, rules and techniques.

Programme Outcomes:
PO1: Ability to understand the concepts of key areas in computer science.
PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society.
PO3: Effective communication and presentation skill.
PO4: Ability to understand professional and ethical responsibility.
PO5: Recognition of the need for life-long learning.

Programme Educational Objectives:
PEO1: To provide a basic foundation in the domain of computer applications.
PEO2: To develop analytical and problem-solving skills for life-long learning in computer science.
PEO3: To provide practical skill of tools and technologies to solve real-world problems.
PEO4: To impart knowledge and inspiration to prepare and pursue further academic studies.
PEO5: To induce the consciousness of ethics and moral values to serve the industry and society.

Unit-1: Cyber Security

Lesson Objective:
To learn about different types of cybercriminals and the motives behind them.

Course Outcome:
CO1

Programme Outcome:
C01

Programme Educational Objectives:
P01, P03

<table>
<thead>
<tr>
<th>Sub Unit</th>
<th>Lesson Duration (Hour)</th>
<th>Summary of Topic</th>
<th>Study Material</th>
<th>Teaching Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1</td>
<td>Basic Terminologies: Cybercrime, Cybersecurity, Cyberspace, Cybersquatting,</td>
<td>NG #1 Page no.</td>
<td>Topic Slide</td>
</tr>
</tbody>
</table>

Ms. Rutu Patel, Ms. Unnati Shah
<table>
<thead>
<tr>
<th>Sub Unit</th>
<th>Lesson Duration (Hour)</th>
<th>Summary of Topic</th>
<th>Study Material</th>
<th>Teaching Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>1</td>
<td>Needs of Cyber Security</td>
<td>NG #1 Page no. 13</td>
<td>Discussion</td>
</tr>
<tr>
<td>1.3</td>
<td></td>
<td>Cyber Criminals: Introduction and Types</td>
<td>NG #1 Page no. 16 - 17</td>
<td>Discussion, Audio visual tool</td>
</tr>
<tr>
<td>1.4</td>
<td>1</td>
<td>Planning Cyber Attacks: Phases and Types</td>
<td>NG #2 Page no. 49 – 61</td>
<td>Topic Slide</td>
</tr>
<tr>
<td>1.5</td>
<td>2</td>
<td>Cybercrimes Classifications</td>
<td>NG #1 Page no. 17 - 22</td>
<td>Topic Slide, MOOC Video</td>
</tr>
</tbody>
</table>

Other References:
- [https://www.coursera.org/learn/cyber-conflicts/lecture/Pp5sl/introduction-to-cyberwarfare](https://www.coursera.org/learn/cyber-conflicts/lecture/Pp5sl/introduction-to-cyberwarfare)

Learner Activities:
**Slow Learner:**
- Write the answers of two questions given by the course teacher.

**Advanced Learner:**
- After the completion of the unit, any five students selected by teacher. Selected student will discuss any one real world example regarding cyber attacked took place during year 2019.

Assessment Parameters:
- Quiz, Unit Test-1, Internal

### Unit-2: Cyber Offenses

**Lesson Objective:**
To gain knowledge about cyber-attacks and prevent them by using different techniques such as strong password, protect identity online, protect computer with security software

**Course Outcome:**
- CO1, CO2

**Programme Outcome:**
- PO1, PO3, PO4

**Programme Educational Objectives:**
- PEO1, PEO3

<table>
<thead>
<tr>
<th>Sub Unit</th>
<th>Lesson Duration (Hour)</th>
<th>Summary of Topic</th>
<th>Study Material</th>
<th>Teaching Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>1</td>
<td>Social engineering: Overview</td>
<td>NG #2 Page no. 61 – 65</td>
<td>Topic Slide</td>
</tr>
<tr>
<td>2.2</td>
<td>2</td>
<td>Cyber stalking: types and method Type: Online stalkers</td>
<td>NG #2 Page no. 66-67</td>
<td>Chalk &amp; Talk</td>
</tr>
</tbody>
</table>

Ms. Rutu Patel, Ms. Unnati Shah
2.3 1  Botnets: Overview  NG #2 Page no. 71-73  Topic Slide

2.4  Attack vectors: Overview  NG #2 Page no. 73-75  Topic Slide

2.5 1  Trends in mobility – types, classification of attacks in 3G mobile networks  NG #3 Page no. 84-86  Discussion

Other References:

Learner Activities:
Slow Learner:
- Write the answers of two questions given by the course teacher.

Advanced Learner:
- After the completion of the unit, any three students selected by teacher. Selected student will discuss any one real world example regarding cyber stalking took place in last five years.

Assessment Parameters:
Quiz, Unit Test-1, Internal
### Prevention

**Types:**
- Financial identity theft
- Criminal identity theft
- Identity cloning
- Business identity theft
- Medical identity theft
- Synthetic identity theft
- Child identity theft

**Techniques:**
- Human-based
- Computer-based

### 3.3 DoS Attack

**Classification:**
- Bandwidth attacks
- Logic attacks
- Protocol attacks
- Unintentional DoS attack

**Types:**
- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- Nuke

### 3.4 DDoS Attack

**Introduction and Prevention**

### 3.5 SQL Injection

**Introduction and Prevention**

### Other References:

### Learner Activities:

**Slow Learner:**
- Write the answers of two questions given by the course teacher.

**Advanced Learner:**
- Any one student selected by course teacher give introduction on SQL Injection.

### Assessment Parameters:
- Unit Test-1, Internal

---

**Unit-4: Cryptography and Digital Signature**

**Lesson Objective:**
To acquire knowledge on cryptography, digital signature and public-key infrastructure in context of cyber security.

**Course Outcome:**
- CO4

**Programme Outcome:**
- PO1, PO3

**Programme Educational Objectives:**
- PEO1, PEO3, PEO4

<table>
<thead>
<tr>
<th>Sub</th>
<th>Lesson</th>
<th>Summary of Topic</th>
<th>Study</th>
<th>Teaching</th>
</tr>
</thead>
</table>

Ms. Rutu Patel, Ms. Unnati Shah
<table>
<thead>
<tr>
<th>Unit</th>
<th>Duration (Hour)</th>
<th>Material</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>1</td>
<td>CIA: Confidentiality, Integrity and Availability</td>
<td>VK #1 Page No-2</td>
</tr>
<tr>
<td>4.2</td>
<td>2</td>
<td>Overview of Symmetric-Key Cryptography</td>
<td>VK #2 Page No-15-17</td>
</tr>
<tr>
<td>4.3</td>
<td>2</td>
<td>Overview of Asymmetric-Key Cryptography</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>1</td>
<td>Hash Functions: Overview and Usage</td>
<td>VK #9 Page No-222-223</td>
</tr>
<tr>
<td>4.5</td>
<td>1</td>
<td>Digital Signature: Introduction and Importance</td>
<td>VK #10 Page No-241-243</td>
</tr>
</tbody>
</table>

**Other References:**
- https://www.coursera.org/learn/basic-cryptography-and-crypto-api/lecture/1W0Os/course-overview

**Learner Activities:**
- **Slow Learner:**
  - Write the answers of two questions given by the course teacher.
- **Advanced Learner:**
  - After the completion of the unit, students solve the case study given by the course teacher.

**Assessment Parameters:**
- Unit Test-2, Internal

**Unit-5: Legal Perspectives of Cyber Security**

**Cross Linkage:** 4.2, 4.3, 4.5

**Lesson Objective:**
To familiar the cyber laws against cyber crime, especially in the Indian context.

**Course Outcome:**
CO2, CO4, C05

**Programme Outcome:**
PO1, PO3, PO4, PO5

**Programme Educational Objectives:**
PEO1, PEO5

<table>
<thead>
<tr>
<th>Sub Unit</th>
<th>Lesson Duration (Hour)</th>
<th>Summary of Topic</th>
<th>Study Material</th>
<th>Teaching Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>1</td>
<td>Need of Cyber Laws: Reasons for Enactment of Cyber Laws in India</td>
<td>NG #6 - Page No. 253 – 254</td>
<td>Discussion</td>
</tr>
<tr>
<td>5.2</td>
<td></td>
<td>Indian ITA: ITA Sections</td>
<td>NG #6 - Page No. 254 – 263</td>
<td>Topic Slide</td>
</tr>
<tr>
<td>5.3</td>
<td>2</td>
<td>Digital Signature and ITA: Public Key Certificate</td>
<td>NG #6 - Page No. 273</td>
<td>Topic Slide, Case Study</td>
</tr>
<tr>
<td>5.4</td>
<td>1</td>
<td>Representation of Digital Signatures in ITA</td>
<td>NG #6 - Page No. 274 – 275</td>
<td>Topic Slide</td>
</tr>
</tbody>
</table>

Ms. Rutu Patel, Ms. Unnati Shah
### Unit-6: Cyber Forensics Fundamentals

**Cross Linkage:** 5.1, 5.2

**Lesson Objective:**
To aware about the importance of digital forensics with its phases, rules and techniques.

**Course Outcome:**
CO2, CO6

**Programme Outcome:**
PO1, PO4, PO5

**Programme Educational Objectives:**
PEO1, PEO3, PEO5

<table>
<thead>
<tr>
<th>Sub Unit</th>
<th>Lesson Duration (Hour)</th>
<th>Summary of Topic</th>
<th>Study Material</th>
<th>Teaching Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>1</td>
<td>Needs</td>
<td>NG #7- Page No. 323–327</td>
<td>Discussion</td>
</tr>
<tr>
<td>6.2</td>
<td></td>
<td>Computer Forensics and Digital Forensics</td>
<td>NG #7- Page No. 320–323</td>
<td>Topic Slide</td>
</tr>
<tr>
<td>6.3</td>
<td>1</td>
<td>Role of Digital Forensics</td>
<td>NG #7- Page No. 327–331</td>
<td>Discussion</td>
</tr>
<tr>
<td>6.4</td>
<td></td>
<td>Rules of Evidence</td>
<td>NG #7- Page No. 339–353</td>
<td>Topic Slide</td>
</tr>
<tr>
<td>6.5</td>
<td>2</td>
<td>Digital Forensics Phases</td>
<td>NG #7- Page No. 402–403</td>
<td>Discussion, Case Study</td>
</tr>
<tr>
<td>6.6</td>
<td>2</td>
<td>Digital Forensics Techniques</td>
<td>NG #7- Page No. 402–403</td>
<td>Discussion, Case Study</td>
</tr>
</tbody>
</table>

**Other References:**

**Learner Activities:**

**Slow Learner:**
- Write the answers of two questions given by the course teacher.

**Advanced Learner:**
- After the completion of the unit, students solve the case study given by the course teacher.

**Assessment Parameters:**
Internal
Study Material:


The following activities shall be carried out by the teacher.

1. Demonstration of NMAP/SQLmap tool.
2. Demonstration of security settings in personal computer.