

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

### COURSE MODULE FOR THE SESSION 2026(ODD SEMESTER)

#### Course Syllabus with CO's

| <b>Academic Year:- 2026</b>           |                                                 |               |                                                     |                            |   |   |                        |
|---------------------------------------|-------------------------------------------------|---------------|-----------------------------------------------------|----------------------------|---|---|------------------------|
| <b>Department:-CSE-Cyber Security</b> |                                                 |               |                                                     | <b>Faculty:-Darshini Y</b> |   |   |                        |
| Course Code                           | Course Title                                    | Core/Elective | Prerequisite                                        | Contact Hours              |   |   | Total Hrs/<br>Sessions |
|                                       |                                                 |               |                                                     | L                          | T | P |                        |
| BCY515C                               | HACKER TECHNIQUES, TOOLS, AND INCIDENT HANDLING | Elective      | Fundamentals of cyber Security and its applications | 3                          | - | - | 40                     |

#### Objectives:

- To understand ethical hacking, penetration testing and physical security controls.
- To identify the various foot printing and port scanning tools and techniques.
- To study enumeration and wireless vulnerabilities exploited by hackers.
- To learn about common types of malware, Trojans, backdoors, spyware, ransom ware and sniffers.
- To study various incident response and defensive technologies.

#### Topics Covered as per Syllabus

##### Module -1

**Hacking:** The Next Generation: Profiles and Motives of Different Types of Hackers, History of Computer Hacking, Ethical Hacking and Penetration Testing, Common Hacking Methodologies, Performing a Penetration Test, The Role of the Law and Ethical Standards.

**Physical Security:** Basic Equipment Controls, Physical Area Controls, Facility Controls, Personal Safety Controls, Physical Access Controls, Avoiding Common Threats to Physical Security, Defense in Depth.

**Textbook: Chapter 1, Chapter 4**

##### Module -2

**Footprinting Tools and Techniques:** The Information-Gathering Process, The Information on a Company Website, Discovering Financial Information, Google Hacking, Exploring Domain Information Leakage, Tracking an Organization's Employees, Exploiting Insecure Applications, Using Social Networks, Using Basic Countermeasures.

**Port Scanning:** Determining the Network Range, Identifying Active Machines, Mapping Open Ports, OS Fingerprinting, Mapping the Network, Analyzing the Results.

**Textbook: Chapter 5, Chapter 6**

##### Module -3

**Enumeration and Computer System Hacking:** Windows Basics, Commonly Attacked and Exploited Services, Enumeration, System Hacking, Types of Password Cracking, Using Password Cracking, Using PsTools, Rootkits, Covering Tracks.

**Wireless Vulnerabilities:** The Importance of Wireless Security, Working with and Securing Bluetooth, Working with Wireless LANs, Threats to Wireless LANs, Internet of Things (IoT), Wireless Hacking Tools, Protecting Wireless networks.

**Textbook: Chapter 7, Chapter 8**

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

### Module -4

**Malware:** Malware, Viruses and How they Function, Worms and How they Function, Significance of Trojans, Detection of Trojans and Viruses, Trojan Tools, Distribution Methods, Trojan Construction Kits, Backdoors, Covert Communication, Spyware, Adware, Scareware, Ransomware.

**Sniffers, Session Hijacking, and Denial of Service Attacks:** Sniffers, Session Hijacking, Distributed Denial of Service (DDoS) Attacks, Botnets and the Internet of Things (IoT).

### Module -5

**Incident Response:** What is Security Incident? The Incident Response Process, Incident Response Plans, Planning for Disaster and Recovery, Evidence Handling and Administration, Requirements of Regulated Industries.

**Defensive Technologies:** Defense in Depth, Intrusion Detection Systems, The Purpose of Firewalls, Honeypots / Honeynets, The Role of Controls, Security Best Practices.

**Textbook: Chapter 14, Chapter 15**

### Textbooks:

1. Sean-Philip Oriyano, Michael G Solomon "Hacker Techniques, Tools, and Incident Systems", Third Edition, Jones & Bartlett Learning, 2020.

### Reference Books:

1. Abhinav Ojha, "Beginners Guide to Ethical Hacking and Cyber Security", Notion Press, 2020.
2. Hugo Hoffman, "Ethical Hacking with Kali Linux - Learn Fast how to Hack like a Pro", 2020.

### List of URL's:

- <https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about>
- <https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks>
- <https://www.youtube.com/watch?v=mOOIv8-IuEo>
- <https://www.youtube.com/watch?v=R0up9SZJqyQ>
- <https://archive.nptel.ac.in/courses/106/105/106105217>.

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY

**Course outcomes:** The students should be able to:

- Explain hacking and penetration testing, including ethical and legal implications and identify basic equipment controls, physical area controls, and facility controls.
- Identify common information gathering tools and techniques and analyze how port scanning and fingerprinting are used by hackers.
- Analyze how enumeration is used in conjunction with system hacking and analyze wireless network vulnerabilities exploited by hackers.
- Identify common types of malware, Trojans, backdoors, and covert communication methods.
- Perform incident handling by using appropriate methods, compare and contrast defensive technologies.

**Internal Assessment Marks: 40 (3 Session Tests are conducted during the semester and Marks allotted based on average of 2 performances and sum of 2 Assignments will be out of 100 marks and will be scaled down to 50 marks)**

### The Correlation of Course Outcomes (CO's) and Program Outcomes (PO's)

| Subject Code            | BCY515C |     |     |     |     | Title: Hacker Techniques, Tools, and Incident Handling |     |     |     |      |      |       |
|-------------------------|---------|-----|-----|-----|-----|--------------------------------------------------------|-----|-----|-----|------|------|-------|
| List of Course Outcomes | PO 1    | PO2 | PO3 | PO4 | PO5 | PO6                                                    | PO7 | PO8 | PO9 | PO10 | PO11 | Total |
| CO-1                    | 2       | 3   | 2   | -   |     | -                                                      | -   | -   | -   | -    | 2    | 9     |
| CO-2                    | 2       | 3   | 2   | -   | 3   | -                                                      | -   | -   | -   | -    | 2    | 12    |
| CO-3                    | 2       | 3   | 2   | -   | 3   | -                                                      | -   | -   | -   | -    | 2    | 12    |
| CO-4                    | 2       | 3   | 2   | -   | 3   | -                                                      | -   | -   | -   | -    | 2    | 12    |
| CO-5                    | 2       | 3   | 2   | -   |     | -                                                      | -   | -   | -   | -    | 2    | 09    |
| <b>Total</b>            | 10      | 15  | 10  | -   | 9   | -                                                      | -   | -   | -   | -    | 10   | 54    |

### The Correlation of Program Specific Outcome's (PSO's) and Course Outcome (CO's)

| Subject Code             | BCY515C | Title: Hacker Techniques, Tools, and Incident Handling |       |
|--------------------------|---------|--------------------------------------------------------|-------|
| List of Course Outcome's | PSO1    | PSO2                                                   | Total |
| CO-1                     | -       | 3                                                      | 3     |
| CO-2                     | -       | 3                                                      | 3     |
| CO-3                     | -       | 3                                                      | 3     |
| CO-4                     | -       | 3                                                      | 3     |
| CO-5                     | -       | 3                                                      | 3     |
| <b>Total</b>             | -       | 15                                                     | 15    |

**Note:** 3 = Strong Contribution 2 = Average Contribution 1= Weak Contribution - = No Contribution