



**Logic Finder**  
Consulting, Development and Training

## Introduction to Cybersecurity Tools and Cyber Attacks

Instructor Led Live Virtual Class

Duration: 6 Day (20-30 hours) | Course Number: LF-Introduction to Cybersecurity Tools and Cyber Attacks -200

### Course outline/Syllabus:

**Week 1:** Introduction to Cybersecurity

**Theory:** Understanding Cybersecurity, its importance, and basic terminologies.

**Practical:** Setting up a safe and secure lab environment for cybersecurity practices.

**Week 2:** Understanding Cyber Attacks

**Theory:** Types of cyber attacks (like phishing, malware, etc.) and their impact.

**Practical:** Recognizing and analyzing phishing emails.

**Week 3:** Fundamentals of Network Security

**Theory:** Basics of computer networks and their vulnerabilities.

**Practical:** Setting up and securing a basic home/office network.

**Week 4:** Introduction to Cryptography

**Theory:** Principles of cryptography and its role in cybersecurity.

**Practical:** Implementing basic encryption and decryption techniques.

**Week 5:** Security Protocols and Measures

**Theory:** Overview of security protocols (SSL/TLS, HTTPS, etc.).

**Practical:** Configuring SSL certificates on a website.

**Week 6:** Operating System and Application Security

**Theory:** OS vulnerabilities, patch management, and secure configurations.

**Practical:** Securing an operating system (Windows/Linux).

**Week 7:** Introduction to Ethical Hacking

**Theory:** Ethical hacking basics, laws, and ethics.

**Practical:** Reconnaissance techniques and tools.

**Week 8:** Malware and Its Analysis

**Theory:** Understanding different types of malware.

**Practical:** Basic malware analysis and identification tools.

**Week 9:** Network Defense Strategies

**Theory:** Firewall, IDS/IPS, and network segmentation.

**Practical:** Setting up and configuring a basic firewall.

**Week 10:** Security Information and Event Management (SIEM)

**Theory:** Introduction to SIEM solutions and their importance.

**Practical:** Basic usage of a SIEM tool (like Splunk).

**Week 11:** Incident Response and Disaster Recovery

**Theory:** Steps of incident response, creating a disaster recovery plan.

**Practical:** Drafting an incident response plan for a hypothetical scenario.

**Week 12:** Capstone Project and Review

**Practical Project:** A comprehensive project covering all aspects learned.

**Review:** Recap of key concepts and open Q&A session.

**Each week should ideally include:**

**Lectures:** To cover theoretical aspects.

**Lab Sessions:** For hands-on experience with tools and techniques.

**Assignments and Quizzes:** To reinforce learning and assess progress.

**Additional Elements**

**Guest Lectures:** Inviting cybersecurity professionals to share real-world experiences.

**Online Resources:** Providing access to online resources, forums, and communities for extended learning.

**Continuous Assessment:** Regular quizzes and assignments to gauge understanding and progress.