Training Orientation Day Report
Date: 17 June 2025
Mode: Online
Session Type: Orientation
Organized By: E&ICT Academy, IIT Kanpur

Overview of the Orientation Session

The orientation session marked the beginning of the Ethical Hacking Training program organized by IIT Kanpur. The session was conducted online and aimed to introduce us to the course structure, training modules, and virtual lab setup. We were also guided on how to make the most of the sessions through active participation and lab practice.

Topics Discussed

1. Training Objectives and Outcomes

- Understand core principles of cybersecurity and ethical hacking
- Gain hands-on skills in penetration testing, malware analysis, and more
- Prepare for CEH (Certified Ethical Hacker)-aligned knowledge

2. Module Overview

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning & Vulnerability Assessment
- Enumeration
- System Hacking
- Malware
- DoS
- Session Hijacking
- Wireless Hacking
- And more advanced topics

3. Virtual Lab Environment

- Platforms: VMware with Kali Linux, Windows 10/11, Ubuntu
- Tools to be used: Nmap, Wireshark, Burp Suite, Metasploit, Aircrack-ng, etc.
- Emphasis on isolating virtual machines for malware handling

4. Participation Guidelines

- Attendance protocol
- Assignment and lab submission procedure
- Daily reporting expectations

Key Takeaways

- Understood the importance of a secure, controlled lab environment for ethical hacking
- Familiarized with the tools and platforms we will use throughout the course
- Got a clear view of the training schedule and learning path
- Realized the scope of ethical hacking in real-world cybersecurity careers

---

Additional Notes

- Training portal and timetable links were provided
- Trainers emphasized the need for maintaining daily reports and active participation

Training Day 2 Report
Date: 6 June 2024
Module Name: Introduction to Information Security
Mode: Online
Instructor: [Insert Trainer's Name]

Main Focus of the Module

The second day of training focused on building a foundational understanding of **Information Security**. The session covered key theoretical concepts such as the **elements of information security**, types of **cyberattacks**, and the **vulnerabilities** that make systems prone to these attacks. We also explored how modern warfare has shifted to **information warfare**, and the distinction between **offensive** and **defensive cyber strategies**.

Topics Covered

1. Information Security Overview

- Ensures confidentiality, integrity, and availability (CIA Triad)
- Aims to protect data from unauthorized access, disclosure, disruption, or destruction

2. Elements of Information Security

- **Confidentiality** – Protecting sensitive data from unauthorized access
- **Integrity** – Ensuring data is accurate and unaltered
- **Availability** – Ensuring systems/data are accessible when needed
- **Authentication & Authorization** – Verifying identity and access rights
- **Non-repudiation** – Preventing denial of actions performed

3. Types of Attacks

- **Active Attacks** – Modify or destroy data (e.g., DoS, spoofing)
- **Passive Attacks** – Monitor data without altering it (e.g., sniffing)
- **Insider vs Outsider Attacks** – Origin of threat
- **Targeted vs Opportunistic Attacks** – Focused vs random attacks

4. Vulnerability and Its Causes

- **Definition:** A weakness in system design, configuration, or coding
- **Reasons for Vulnerability:**
  - Human errors
  - Unpatched software
  - Weak passwords
  - Misconfigured systems
  - Lack of security policies

5. Classification of Attacks

- **Network Attacks:** Sniffing, spoofing, DoS
- **Application Attacks:** SQL injection, XSS
- **Physical Attacks:** Theft of devices
- **Social Engineering:** Phishing, baiting, pretexting

6. Information Warfare

- Use of digital tools to gain advantage over adversaries
- Disruption of communications, misinformation, and system compromise

7. Defensive vs Offensive Cyber Warfare

- **Defensive Warfare:** Firewalls, IDS/IPS, patching, access control
- **Offensive Warfare:** Penetration testing, ethical hacking, red teaming
- Governments and organizations now invest in both strategies to prepare for cyber conflict

---

Key Takeaways

- Understood the core principles and pillars of information security
- Realized how even small vulnerabilities can lead to major data breaches
- Gained clarity on how attacks are classified and how modern warfare includes cyber dimensions
- Identified the growing need for both **proactive defense** and **controlled offensive security** in the cybersecurity landscape