MODCOM Institute of Technology

🏢 Lesson 9: Introduction to Ethical Hacking

Module 14: Ethical Hacking Principles
Topic: What is Ethical Hacking?

⏱️ **Duration:** 3 hours
🧠 **Objective:** Understand the role and importance of ethical hacking in cybersecurity as well as legal and ethical boundaries of hacking and the importance of compliance.

🧩 Session Breakdown

1. 🧭 Introduction (30 mins)

- Icebreaker: "What comes to mind when you hear the word hacker?"
- Define hacking and its types (white-hat, black-hat, gray-hat)
- Real-world ethical hacker case studies (e.g., Kevin Mitnick, bug bounty programs)

2. 🛠️ Legal & Regulatory Compliance in Ethical Hacking

- Discussion: "What could go wrong if a penetration test is conducted without permission?"
- Overview of laws and regulations:
    - **Computer Misuse Act (Kenya)**
    - **CFAA (USA)**
    - **GDPR (EU)**
    - **HIPAA, PCI-DSS, and others**
- Ethical hacking certifications and codes of conduct (EC-Council, CompTIA)

3. 🛠️ Practical Session (1 hour 30 mins)

- **Activity 1:** Analyze a case study of legal vs illegal hacking (e.g., Equifax breach vs bug bounty programs)
- **Activity 2:** Break into teams and review simplified RoE (Rules of Engagement) documents — identify what's allowed and what's not
- **Lab:** Create a draft RoE and compliance checklist for a fictional pentest project

4. 🎯 Conclusion (30 mins)

- Recap: Ethical vs Unethical hacking
- Discuss: Why organizations need ethical hackers
- Q&A and assignment briefing

📝 Homework/Assignment:

- Write a 1-page reflection: "Why I want to learn ethical hacking and where I plan to use it."