Ethical Hacking Essentials
Provider: EC-Council (Coursera / EdX)
Completion Date: May 2, 2025

Overview
This course provided a foundational yet hands-on introduction to ethical hacking concepts, threats, and countermeasures across a wide range of attack surfaces. It combined video lectures, scenario-based instruction, and real-world lab environments to help students understand how hackers exploit vulnerabilities—and how to ethically counter those techniques.

Topics included information security threats, password cracking, social engineering, network and wireless attacks, web application hacking, mobile and IoT/OT exploitation, cloud computing threats, and S3 bucket misconfigurations. Labs were conducted in isolated environments using tools such as SET, PhishTank, Wireshark, Metasploit, and AWS CLI (where possible), reinforcing the practical aspects of each topic.

Key Topics Covered

- Information security principles and hacker types
- Threat modeling, vulnerability assessment, and risk management
- Password cracking methods and brute-force/dictionary defenses
- Social engineering, phishing, and user-targeted deception
- Network sniffing, ARP poisoning, and DDoS (hping3, HOIC)
- Session hijacking, MAC flooding, and detection with Wireshark
- Web application attacks (XSS, SQLi, command injection)
- Wireless attack simulation (WEP key cracking, beacon flooding)
- Mobile attack simulation (Android payloads using msfvenom)
- IoT and OT exploitation footprinting using Shodan
- Public S3 bucket enumeration and exploitation with AWS CLI

Lab Summaries

Lab work was completed for most modules, with the following highlights:

- **Social Engineering Techniques:** Simulated phishing site via SET (unsuccessful clone), analyzed real phishing domains via PhishTank, and discussed ethical limits of offensive simulation.

- **Network Level Attacks:** Conducted ARP poisoning, DoS and DDoS attacks (hping3, HOIC), detected attacks via Wireshark and ARP spoofing detection.
- **Wireless Attacks:** Attempted WEP cracking using airodump-ng and aireplay-ng; packet threshold not met in the lab environment, demonstrating real-world limitations.
- **Web Application Attacks:** Demonstrated command injection and SQL injection vulnerabilities; accessed server files and verified output tampering.
- **Mobile Attacks:** Lab incomplete due to oversized Android emulator UI and APK interaction limitations; payload creation attempted but not executed.
- **IoT & OT Attacks:** Performed open-source footprinting techniques; Shodan portion skipped due to account requirement.
- **Cloud Computing Threats:** LazyS3 enumeration encountered environment mismatch; AWS CLI lab skipped due to AWS login requirement.

Incomplete Labs (by choice or limitation)

- Android emulator exploit (APK install failed)
- Shodan-based IoT enumeration (account required)
- AWS S3 bucket exploitation via CLI (account required)

These labs were consciously left incomplete due to system limitations, ethical boundaries, or refusal to create third-party accounts for lab-only purposes. No data was extracted or manipulated during those tasks.

Reflection

This course significantly deepened my understanding of how real-world attackers operate across physical, network, application, and cloud-based vectors. While I encountered technical limitations in a few lab environments, I completed all hands-on tasks where platform access allowed, and I made conscious decisions not to perform simulations that required account creation or unsupported mobile interfaces.

The content in this course solidified my core competency in ethical hacking and red-team awareness, preparing me to move forward in advanced penetration testing, cybersecurity compliance, and digital forensics.