Pen Testing, Threat Hunting, and Cryptography

**Provider:** IBM (Coursera)

**Completion Date:** August 25, 2025

**Overview**

This course focused on the core techniques used in ethical hacking, threat intelligence, and cryptography. Learners practiced penetration testing from planning through reporting using real tools and attack scenarios. The course included threat intelligence frameworks and encryption methods that support modern cybersecurity operations.

**Key Topics Covered**

- Penetration testing phases: planning, discovery, attack, reporting
- Reconnaissance techniques: passive and active
- Tools: Nmap, ZAP, SNYK, Google Dorking, IBM X-Force Exchange
- Threat intelligence platforms and SIEM systems
- Cryptographic principles: AES, RSA, hashing, key management
- Final project: real-world scenario with pen test plan and report

**Practical Applications**

- Conduct port scans and recon using real tools
- Create a penetration testing report using PTES format
- Identify vulnerabilities in code and systems
- Use threat intelligence feeds to assess risk
- Apply encryption and hashing to secure sensitive data

**Personal Reflection**

This course tied together the red team side of cybersecurity with practical reporting and threat intel skills. It built on earlier technical classes and gave me a strong foundation for assessing vulnerabilities, performing structured tests, and defending against threats. It also pushed me to think like an attacker in order to strengthen my defense approach.