Cybersecurity & Ethical Hacking Track Overview

Comprehensive Understanding & Practical Application

Your Name

Source: Ethical Hacking Pictures | Unsplash

Program Goal & Core Topics

Our Program Goal: Holistic Cybersecurity Mastery

- Provide a comprehensive understanding of cybersecurity concepts and their real-world applications.
- Equip participants with proficiency in ethical hacking tools for web application security.
- Foster expertise in cryptography and incident response, culminating in a practical Security Audit Report.

Core Topics Overview

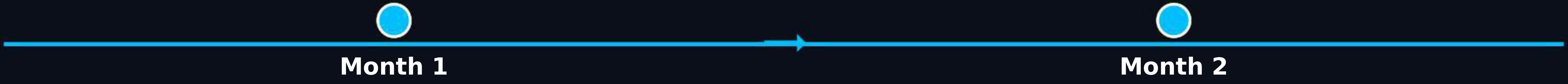
Introduction to

Network Security

VAPT

Ethical Hacking Tools

Phase 1: Foundational & Core Concepts (Months 1 & 2 - Online)



Month 1: Fundamentals & Defense

- **Cybersecurity Concepts:** Intro to Threats, the CIA Triad, and practical Lab Setup.
- **Network Security:** Explore OSI/TCP/IP, common attacks, and defensive tools like IDS/IPS.
- **Cryptography:** Basics of Encryption, Hashing, and PKI.
- **Reconnaissance Tools:** Learn OSINT, Nmap scans, and vulnerability scanners.

Month 2: Offensive & Defensive

- **Web App Security:** Dive into the OWASP Top 10, covering Injection & XSS.
- **Exploitation:** Hands-on with the Metasploit Framework to gain access.
- **Post-Exploitation:** Use Meterpreter, crack passwords, and create professional reports.
- **Incident Response:** Understand the IR Lifecycle and basics of Digital Forensics.

Hands-on Learning: Practical Skills Development

Cybersecurity Fundamentals

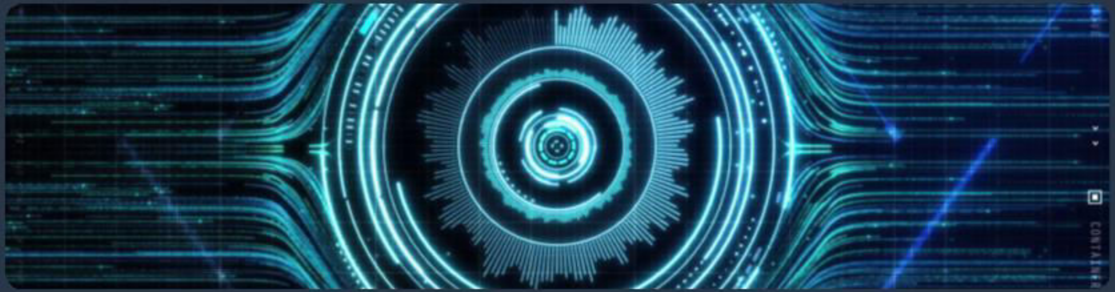
Navigating Kali Linux: Gain proficiency in the industry-standard distribution for penetration testing.
Basic Command-Line: Master fundamental Linux commands crucial for automation and tool interaction.

Linux Proficiency | Command-Line

Network Security

Firewall Configuration: Implement policies to control traffic and protect network perimeters.
Wireshark Analysis: Develop skills in packet capture to identify anomalies and detect threats.

Traffic Filtering | Packet Inspection



Cryptography

OpenSSL Usage: Apply OpenSSL for data encryption, decryption, and managing digital certificates.
Hash Generation: Create cryptographic hashes for data integrity verification and secure storage.

Data Secrecy | Data Integrity

Ethical Hacking

Utilize **Nmap** for scans, **Burp Suite** for web requests, and **Metasploit** for exploitation & post-exploitation activities.

Reconnaissance | Exploitation | Web Pen Testing

Phase 2: Industry Immersion & Integrated Project (Month 3 - Offline)

Week 9: Project Kick-off & Planning

This initial phase focuses on integrating participants into the offline environment, facilitating team formation for the Capstone Mini Project, and assigning dedicated mentors to guide their progress.

The core of Week 9 is the meticulous planning of the 'Security Audit Report'. Participants define project scope, establish clear objectives, and formulate a robust methodology, simulating real-world security assessment engagements.

Practical application commences with in-depth training on advanced security tools like Burp Suite Professional and automated scanners like Nessus or OpenVAS for comprehensive assessments.

Week 10: Advanced VAPT & Professional Reporting

Week 10 progresses to hands-on, in-depth Vulnerability Assessment and Penetration Testing (VAPT) exercises conducted within realistic simulated environments, allowing for practical application of advanced techniques.

Participants will leverage industry-standard tools—Nmap for network reconnaissance, Metasploit for sophisticated exploitation, and Burp Suite for identifying and exploiting web application vulnerabilities.

The week culminates in developing effective vulnerability remediation strategies and crafting professional-grade security audit reports, focusing on clear communication of findings, risk, and recommendations.

Simulated Incident Response & Project Showcase

Week 11

Week 11: Simulated Incident Response & Digital Forensics

Engage in realistic cyber incident simulations designed to mirror real-world threats, providing invaluable hands-on experience in a controlled environment.

Full Incident Response Lifecycle:

- Identification
- Containment
- Eradication
- Recovery

Develop fundamental skills in analyzing logs, network captures (Wireshark), and system artifacts to reconstruct events.

Live Simulation · IR Lifecycle Mastery · Log Analysis · Evidence Collection

Week 12: Project Showcase & Career Launchpad

Culminate your learning with a comprehensive 'Security Audit Report' presentation to a distinguished panel of industry experts, simulating a professional client engagement.

The Capstone Mini-Project: Security Audit Report

Comprehensive Security Audit

Defining the Engagement

Detailed 'Security Audit Report': Student work on a comprehensive report for a simula organization, mirroring real-world security engagements.

Defining Scope: Clearly outline the bounda of the audit, including specific systems, networks, or applications to be assessed for focused evaluation.

Establishing Methodology: Employ industry-standard processes like VAPT to systematically identify security flaws using both automated tools and manual techniques.

Producing Deliverables: Generate a professional report detailing vulnerabilities, risks, and actionable remediation recommendations.

- Scope Definition
- Methodology Driven
- Risk Assessment
- Remediation Planning

Practical Application

Integrated Skills for Real-World Impact

Skill Integration: This project provides a holistic application of theoretical knowledge, teaching students to combine various techniques effectively.

From Reconnaissance to Reporting: The project covers the entire cybersecurity lifecycle:

- Reconnaissance
- Vulnerability Assessment
- Exploitation
- Professional Reporting

Real-world Preparedness: The hands-on scope prepares students for complex cybersecurity challenges, building confidence and practical expertise.

- Hands-on Experience
- Skill Synthesis
- Career Readiness
- Challenge Simulation

Career Launchpad & Next Steps

Career Development Workshops

Resume & Portfolio Building: Master crafting compelling resumes and robust portfolios that highlight your technical skills and project experience.

Industry Certifications Overview: Gain insight into key certifications like CompTIA Security+, CEH, and OSCP to advance your career.

Professional Branding · Skill Showcasing · Certification Pathways

Interview Preparation

Mock Technical Interviews: Engage in realistic technical interviews to test your knowledge and receive constructive feedback.

Behavioral Interviews: Practice articulating your experiences and skills to align with cybersecurity role demands.

Cybersecurity Scenarios: Discuss practical scenarios to demonstrate critical thinking and incident response capabilities.

Technical Acumen · Problem Solving · Confidence Building

Networking Opportunities

Dedicated Sessions: Connect with leading cybersecurity professionals, industry experts, and hiring managers in

Certification & Recognition

Program Completion Certificate: Receive formal