Coincent 3-Year Program in Cyber Security and Ethical Hacking
Partnered by Threat Prism

Year 1: Live Industrial Training – Build Your Foundation

Gain hands-on industry exposure from day one with 2.5 months of live training in a professional environment. Learn the latest tools and technologies through skill-focused sessions, guided by expert mentors from the industry

Cyber Security and Ethical Hacking Curriculum

Module 1: Networking Basics

Objective: Understand how computer networks function, focusing on key terminology and protocols.

Topics:

- **Types of Networks**: LAN, WAN, MAN, PAN, CAN
- **Basic Terminologies**: IP, MAC, DNS, DHCP, Gateway, Subnet, VPN
- **OSI Model**: 7 layers (Physical to Application); responsibilities of each
- **Protocols**: TCP/IP, UDP, ICMP, HTTP/S, FTP, ARP, DNS, etc.
- **Common Protocols & Ports**:
    - HTTP (80), HTTPS (443)
    - FTP (20/21), SSH (22), Telnet (23)
    - SMTP (25), DNS (53), SNMP (161), RDP (3389)

Module 2: Linux Fundamentals for Hackers

Objective: Use Linux for ethical hacking; master key commands and concepts.

Topics:

- **Installing Kali Linux**: On VM (VirtualBox/VMware) or dual boot
- **Linux Basic Commands**: ls, cd, pwd, cp, mv, mkdir, touch
- **Intermediate Commands**: grep, find, chmod, chown, tar, wget, curl, top
- **Linux Directory & File Permissions**: rwx, chown, chmod, SUID/SGID
- **Linux Utilities**: nmap, netstat, tcpdump, iptables, wireshark

Module 3: Introduction to Ethical Hacking

Objective: Learn the foundational concepts of ethical hacking and information security.

Topics:

- **Information Security Overview**
- **Cyber Kill Chain** (Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command and Control → Actions)
- **Hacking Concepts**: Attack vectors, threat actors
- **Ethical Hacking Concepts**: Legal boundaries, white hat vs. black hat
- **Information Security Controls**: Physical, administrative, technical
- **Information Security Laws and Standards**: GDPR, HIPAA, ISO/IEC 27001

Module 4: Footprinting and Reconnaissance

Objective: Gather information about targets using passive and active techniques.

Topics:

- **Footprinting Methodology**
- **Search Engine Footprinting**: Google dorking
- **Web Services & WHOIS**
- **Social Media Footprinting**
- **DNS & Network Footprinting**
- **Email Tracking & Metadata Analysis**

Module 5: Scanning Networks

Objective: Detect live systems, open ports, services, and OS types.

Topics:

- **Network Scanning Concepts**
- **Scanning Tools**: Nmap, Netcat, Angry IP Scanner
- **Host Discovery**
- **Port and Service Detection**
- **OS Fingerprinting**
- **Bypassing Firewalls/IDS Detection**

Module 6: Enumeration

Objective: Extract more detailed info from discovered hosts.

Topics:

- **NetBIOS Enumeration**
- **SNMP, LDAP Enumeration**
- **DNS, SMTP, NFS, NTP Enumeration**
- **Tools**: enum4linux, snmpwalk, rpcclient, ldapsearch

Module 7: System Hacking

Objective: Understand and simulate unauthorized access to systems.

Topics:

- **System Hacking Concepts**
- **Password Cracking**: Dictionary, Brute-force, Rainbow tables
- **Vulnerability Exploitation**: Using Metasploit
- **Privilege Escalation Techniques**
- **Maintaining Access**: Rootkits, keyloggers
- **Covering Tracks**

Module 8: Denial of Service (DoS)

Objective: Learn DoS/DDoS attack vectors and protection techniques.

Topics:

- **DoS/DDoS Techniques**
- **Botnets**: Architecture and use in attacks
- **Attack Tools**: LOIC, HOIC, hping3
- **Case Studies**: GitHub DDoS, Dyn attack
- **Countermeasures**: Rate limiting, firewalls, CDN

Module 9: IDS, Firewalls, and Honeypots

Objective: Understand and bypass detection systems.

Topics:

- **IDS/IPS/Firewall/Honeypot Concepts**
- **Evading IDS/Firewalls**: Fragmentation, encryption, tunneling
- **Detection Tools**: Snort, Suricata, Wireshark
- **Honeypot Types**: Low-interaction vs. high-interaction
- **Countermeasures**

Module 10: Web Application Hacking

Objective: Exploit and protect web applications.

Topics:

- **Web App Architecture**
- **Threats**: SQLi, XSS, CSRF, LFI, RFI
- **OWASP Top 10 Vulnerabilities**
- **Hacking Tools**: Burp Suite, OWASP ZAP
- **Footprinting & Vulnerability Detection**

Module 11: Wireless Network Hacking

Objective: Understand wireless technologies and exploit weaknesses.

Topics:

- **Wireless Encryption Standards**: WEP, WPA/WPA2/WPA3
- **Attack Techniques**: Evil twin, deauthentication, handshake cracking
- **Tools**: Aircrack-ng, Kismet, Wireshark
- **Bluetooth Hacking**
- **Countermeasures**

Module 12: Mobile Platform Hacking

Objective: Target Android & iOS platforms.

Topics:

- **Attack Vectors**: App vulnerabilities, OS exploits, malware
- **Android Attacks**: APK reverse engineering, ADB access
- **Tools**: MobSF, Drozer, Frida
- **Security Practices**

Module 13: Cryptography

Objective: Learn data encryption and cryptographic security.

Topics:

- **Encryption Types**: Symmetric (AES, DES), Asymmetric (RSA, ECC)
- **Hashing**: SHA, MD5, bcrypt
- **Tools**: GPG, OpenSSL, VeraCrypt
- **Public Key Infrastructure (PKI)**
- **Email & Disk Encryption Techniques**

Year 2: Real-Time Projects – Apply What You've Learned

Transform your knowledge into real-world experience by working on 8 industry-level projects that build your technical and professional skills. Each project enhances your portfolio, strengthening your resume and showcasing your practical abilities. You'll also collaborate in teams, gaining valuable experience in communication, teamwork, and project management—just like in a real work environment.

PROJECTS

Scanning using OWASP ZAP involves identifying vulnerabilities in web applications through automated security testing. ZAP (Zed Attack Proxy) is an open-source tool developed by OWASP that helps in detecting issues like SQL injection, XSS, and insecure authentication. It performs both passive and active scanning by intercepting traffic between the client and server. ZAP is widely used by security analysts for penetration testing, vulnerability assessments, and ensuring compliance with secure coding practices.

Scanning for open ports and attacking them is a common technique in cybersecurity used to identify entry points into a system. Tools like Nmap scan a target machine to detect active ports and the services running on them. Once open ports are discovered, attackers may exploit known vulnerabilities in those services to gain unauthorized access. This method is often used in penetration testing to assess a system's exposure to threats and to harden its defenses.

Information Gathering tools in cybersecurity are used to collect data about a target system, organization, or individual before launching a potential attack or penetration test. These tools help identify domains, IP addresses, subdomains, open ports, technologies used, and even leaked credentials. This phase, also known as reconnaissance, is crucial for mapping the target's surface area and planning further exploitation. It's used by ethical hackers to detect weak points in security.

Exploiting server vulnerabilities in cybersecurity involves taking advantage of weaknesses in a server's software, configuration, or exposed services to gain unauthorized access or control. These vulnerabilities may include outdated software, misconfigured settings, or insecure services like FTP or SMB. Ethical hackers use this process during penetration testing to demonstrate real-world risks and help organizations patch flaws. Exploits can lead to data breaches, privilege escalation, or system takeover if left unaddressed.

OWASP Juice Shop is a deliberately insecure web application developed for learning and practicing web application security. It simulates a real-world e-commerce platform filled with vulnerabilities such as XSS, SQL injection, insecure authentication, and broken access control. Security professionals and students use Juice Shop for hands-on training in ethical hacking and secure coding practices. It's widely used in Capture the Flag (CTF) challenges and cybersecurity education.

System Hacking in the cybersecurity domain refers to the process of gaining unauthorized access to computer systems to uncover vulnerabilities, test defenses, or demonstrate potential risks. It typically involves password cracking, privilege escalation, and accessing sensitive data. Attackers may exploit weak or reused passwords, open ports, or system misconfigurations. Tools like Hydra are used for brute-force attacks on login services, while Auxiliary Modules in Metasploit help in scanning and exploiting services. NSE Scripts in Nmap automate vulnerability

detection and exploitation tasks. John the Ripper is a fast password-cracking tool, and Crunch helps generate custom wordlists for brute-force attacks. These tools are essential for ethical hackers during penetration testing to assess and strengthen system security.

- Tools Utilized:
- Hydra
- Auxiliary Module (Metasploit)
- NSE Scripts (Nmap)
- John the Ripper
- Crunch (Password list generator)

Simulated Ransomware Attack and Defense is a controlled cybersecurity exercise that mimics a real ransomware attack to test an organization's detection and response capabilities. It involves encrypting files or restricting system access in a safe environment to evaluate how security teams react. Defensive measures such as backups, endpoint protection, and incident response are tested. This helps organizations strengthen preparedness and identify gaps in their defenses. It also raises awareness among staff and validates recovery procedures.

Year 3 – Placement & Internship Phase:

In the 3rd year of Coincent's program, students are guaranteed an internship with partner companies, complete with a formal Internship Offer Letter and a Completion Certificate upon successful completion. This internship is a complimentary part of the 3-Year "Industrial Training + Internship" model, which also includes live classes, expert mentorship, and hands-on project work. This phase bridges academic learning with real-world application, providing students with valuable professional exposure before graduation.

Coincent also offers structured placement preparation to ensure students are job-ready. This includes portfolio building through 8 real-time projects, certifications aligned with Microsoft standards, and dedicated training for interviews. From mock interviews to resume reviews and HR/technical round prep, every element is designed to transition students from classroom learning to career success. By the 4th year, students are equipped not just with knowledge, but with experience, credentials, and confidence to enter the workforce.