Ethical Hacking Lab – Systems Security

From security monitoring to hands-on exploitation and incident response

Module overview

This practice-oriented module introduces students to the tools, techniques, and mindset used to analyse attacks and defend modern systems. Students first build a structured foundation in security operations through Cisco's CyberOps course. They then apply and deepen this knowledge in ten in-person labs focused on software exploitation, networking, and Linux kernel security.

By combining guided online learning with hands-on exercises, the module connects defensive security operations with an attacker's perspective—from identifying suspicious activity and investigating evidence to understanding how vulnerabilities are exploited in practice.

Course format and workload

The module awards 6 ECTS credits, corresponding to a total workload of approximately 180 hours. The Cisco CyberOps course is expected to require about 70 hours. The remaining workload covers ten in-person lab sessions, preparation and follow-up, practical assignments, and independent study.

Students who successfully complete the Cisco CyberOps course can also obtain a Cisco certificate, providing recognised evidence of their cybersecurity skills and a valuable addition to their CV.

Part I: Cisco CyberOps (online learning)

The Cisco CyberOps course provides the conceptual and operational foundation for working in a Security Operations Centre (SOC). Its 28 modules are organised around the following themes:

- **Systems and networking fundamentals:** Windows and Linux, network protocols, addressing, transport, services, and infrastructure.
- **Threats and attacker techniques:** Threat actors, reconnaissance, common attacks, attacker tools, and attacks on network and application services.
- **Security controls and resilience:** Defence in depth, access control, cryptography, endpoint protection, and vulnerability assessment.
- **Monitoring and threat intelligence:** Network telemetry, logs, packet analysis, indicators of compromise, threat intelligence, and SIEM data.
- **SOC analysis and incident response:** Alert triage, evidence correlation, digital forensics, containment, recovery, and lessons learned.

Part II: In-person practical labs

Ten lab sessions translate the online material into hands-on security experience. Tentative topics include:

- Assembly debugging
- Heap buffer overflows
- Heap use-after-free vulnerabilities
- Networking fundamentals
- PHP malware analysis
- Introduction to Linux kernel modules
- Root access and rootkits
- UDP communication in Linux kernel modules
- Port handling in Linux kernel modules
- Rootkit analysis and reversal

Assessment and progression requirements

After completing the Cisco CyberOps component, students must pass an examination covering the online course material. Passing this examination is a prerequisite for admission to the in-person practical labs.

The practical labs are assessed on a pass/fail basis and are not graded. To complete the module successfully, students must complete all ten lab exercises and submit a report for each exercise; the reports document successful completion.

Learning outcomes

After completing the module, students will be able to:

- explain how operating systems, networks, and security controls interact in real-world environments;
- recognise common attack techniques and interpret relevant logs, alerts, and network data;
- analyse software vulnerabilities and attacker behaviour using practical tools;
- apply core techniques for alert triage, digital forensics, and incident response; and
- connect offensive experimentation with effective defensive strategies.