CS Academy: Full Curriculum

109 hands-on projects, from first command line to a complete security engagement. Every participant starts with the **Common Core** (29 projects), then specializes in **Blue Team** (defensive security, 35 projects) or **Red Team** (offensive security, 45 projects). Each project is practical: participants work in labs, write scripts, run real security tools and document their findings.

Common Core

29 projects

Getting started Set up the Linux lab, learn Git and core security principles.	1 Cybersecurity Academy Introduction 2 Git - SCM Basics 3 Introduction to Cyber Security
Linux & system security Shell, processes, permissions, SUID/SGID, SELinux and AppArmor.	4 Linux, Shell, basics 5 Linux shell, processes and signals 6 Linux Security Basics 7 Permissions, SUID & SGID 8 Mandatory Access Control
Windows & forensics Windows internals and digital forensics ethics.	9 Windows Fundamentals 10 Forensic Ethics & Methodologies
Networks, crypto & protocols Architecture, hashing, authentication, email and protocol auditing.	11 Networking Foundations & Architecture 12 Cryptography Basics 13 Authentication vs Authorization 14 Email Security Protocols 15 Network Protocols: Auditing and Securing
Reconnaissance & analysis OSINT, Nmap, Python automation and Wireshark.	16 Passive Reconnaissance 17 Active Reconnaissance 18 Nmap Live Host Discovery 19 Python for Cybersecurity 20 Network Traffic Monitoring & Analysis
Web security & vulnerabilities OWASP Top 10, Burp Suite, CVE/CWE/NVD and upload flaws.	21 OWASP Top 10 22 BurpSuite - Fundamentals 23 Content Discovery 24 Understanding Vulnerabilities - Reading 25 CVE, CWE and NVD 26 Upload Vulnerabilities
Governance & careers Threat modeling, security policy and career pathways.	27 Threat Modeling Fundamentals 28 Security Policy Analysis 29 Exploring Career Pathways in Cybersecurity

Specialization: Blue Team

Defensive security | 35 projects

Assess & plan Assess an organization's posture, threats and vulnerabilities, then build a defense strategy.	1 The First Watch 2 Know Your Enemy 3 The Weak Links 4 The Defense Blueprint 5 The Cryptographic Foundation 6 The Board Briefing
Harden systems Linux and Windows hardening, patching, network defense, one deployable package.	7 Locking the Gates 8 The Windows Fortress 9 Eyes on the Endpoint 10 The Patch Equation 11 Perimeter and Network Defense 12 The Defensible Endpoint Package
Detect & triage Evidence pipelines, baselines, Sigma detections, Wazuh SIEM and a 24-hour SOC shift.	13 Evidence Pipeline 14 Reading the Noise 15 The Alert Factory 16 Triage Shift 17 Cross-Platform Detection Analysis 18 The 24-Hour Watch
Investigate & hunt Phishing, packet forensics, threat intel, malware analysis and attack reconstruction.	19 Phishing Dissection 20 Wire Shark Territory 21 Intelligence-Driven Defense 22 Malware Awareness 23 Threat Hunting 24 Attack Reconstruction
Respond & recover Incident response frameworks, containment, forensics and the capstone breach.	25 When the Alarm Sounds 26 Contain and Control 27 The Evidence Trail 28 Lessons Learned 29 The Tabletop 30 The Breach
Govern & automate Compliance, disaster recovery, IAM, SOC automation and human defense.	31 The Compliance Engine 32 When Everything Fails 33 Identity at Scale 34 The SOC Playbook 35 Security Awareness & Human Defense

Specialization: Red Team

Offensive security | 45 projects

Foundations & legal Offensive vs defensive security, contracts, rules of engagement, pentest methodology, risk.	1 Offensive vs Defensive Security 2 Legal and Contractual Aspects 3 Pentesting Contracts 4 Introduction to Penetration Testing 5 Understanding Vulnerabilities (Exploitation) 6 Risk Assessment & Mitigation Strategies
Recon & scanning OSINT, web basics, advanced Nmap, Nessus and enterprise network pentesting.	7 OSINT Profile Builder 8 Web Fundamentals 9 Advanced Network Enumeration with Nmap 10 Nessus 11 Pentest Networking
Web & application exploitation Injection, XSS, IDOR, SSRF, file inclusion and memory corruption.	12 What is the shell? 13 SQL, noSQL Injection 14 XSS 15 Insecure Direct Object Reference 16 Server-Side Request Forgery 17 File Inclusion 18 Command Injection (CVE-2021-44228 Explained) 19 Buffer overflow 20 Advanced Web Attack Techniques
Metasploit & scripting The Metasploit Framework and Ruby scripting for security tools.	21 Metasploit - Basic 22 Ruby Scripting (Cyber) 23 Metasploit - Scripting
Active Directory Enumeration, Kerberos attacks, LDAP, BloodHound and PowerView.	24 Active Directory - Fundamentals 25 Active Directory - Enumeration & Credential Abuse 26 Active Directory - LDAP 27 Active Directory - BloodHound Attack Path Analysis 28 Active Directory - PowerView
Privilege escalation & persistence Gaining root/admin on Linux and Windows and keeping access.	29 Linux Privilege Escalation 30 Windows Privilege Escalation 31 Access Persistence Techniques
Reverse engineering & mobile ELF binaries, static/dynamic analysis, malware, Android apps with Frida.	32 Reverse Engineering Fundamentals 33 Static Analysis in Reverse Engineering 34 Dynamic Analysis in Reverse Engineering 35 Malware Analysis in Reverse Engineering 36 Mobile Application Fundamentals and Security 37 Static Analysis In Mobile Security 38 Dynamic Analysis In Mobile Security
Red team operations & reporting C2 infrastructure, adversary simulation, physical and social engineering, IR, reporting.	39 Red Team Infrastructure & Covert Communications 40 Adversary Simulation Planning 41 Physical Penetration Testing 42 Social Engineering Operations 43 Web Application Fast Incident Response 44 Web Application Forensics 45 Penetration Test Reporting and Remediation

Blue Team projects follow one continuous scenario: protecting a fictional healthcare organization from assessment and hardening to a full breach investigation. All offensive techniques are practiced only in authorized, controlled lab environments, with a strong focus on legal and ethical responsibility.

More than an Academy, a whole learning experience

The learning experience goes beyond the 109 hands-on projects. Participants also get opportunities to connect with the Luxembourg cybersecurity ecosystem through talks with industry professionals and companies, organized workshops, hackathons, and outdoor events. These activities encourage networking, collaboration, knowledge sharing, and community building, giving participants the chance to develop skills and connections.