



Certified Hands-On Cybersecurity Specialist + AI (CHCSS)

————— Syllabus 2025

Interested?

info@trivian.nl | Boeing Avenue 254, 1119 PZ Schiphol-Rijk

Description

A practical entry-level cyber course designed for those looking to enter the field of information security and cyber, or for individuals seeking a career change.

Students will be introduced to a wide range of topics, defense and attack methods from the world of cyber, and will practice using specialized labs and real-world simulation tools — essential for cyber defense professionals working in today's evolving security landscape.

This exclusive training program is offered by Trivian under official license, and was originally developed within top-level security services. It is normally reserved for elite cybersecurity specialists, but now available through Trivian for broader professional development.

The course covers key industry-required topics with a strong focus on hands-on cybersecurity defense skills. Students also train with a custom-built cyber simulator that mimics real-world attacks, enabling them to build practical experience in a high-pressure training environment.

The program is divided into three main parts:

Introduction to Cyber - includes international LPI Linux Essentials (010-160) certification.

Practical Cyber Defense Specialist - taught using advanced cyber labs and simulations.

AI Cyber - focuses on exploiting vulnerabilities, hacker methods, AI-based attack techniques, and how to defend against them.

Target Audience

This course is intended for anyone wishing to learn cybersecurity and enter the cyber domain — whether starting out or changing careers.

Prerequisites

- Basic familiarity with Windows environments
- Technical level of English reading

Cyber Security Specialist

01

Linux Essentials (98 hours)

Subject	Description
LPI Exam and Virtual Machine	<ul style="list-style-type: none">- LPI Exam- Computer Hardware: Introduction- Benefits of Virtualization- Virtualization type- Virtualizing Players - VMware \ Hyper-V \ VirtualBox- Demo - Using VMware Workstations
The Linux Operating System	<ul style="list-style-type: none">- Introducing Linux- Why Linux?- Linux for Desktop- Open Source Licensing Models- History of Linux- Linux Hardware System- OS Commercial Restrictions- The Linux Layers- Software Package Manager- Linux Distribution Families- Linux in Cloud- Linux for Cloud- Long-Term Support (LTS)- Introduction to Linux Installation- Installation-time Decisions- Installing Ubuntu: Pre-Installation Steps- Min. System Requirements
Configuring the Linux Environment	<ul style="list-style-type: none">- Introduction to the Linux Environment- Managing Linux Startup- The Linux File System Hierarchy Standard- Relative and Absolute modes- Learn and practice basic Linux commands

Configuring the Linux Desktop Experience

- Working with Linux Software Repositories
 - Exploring Linux Desktop Applications
 - Understanding Linux Desktops
-

Working with Linux Command Line Basics

- Using Linux Help Resources
 - The Linux Terminal
 - Linux Command Syntax Patterns and Shortcuts
-

Navigating the Linux File System

- Working with Files and Directories
 - Searching the Linux File System
 - Working with Archives
 - Linux Kernel Modules and Peripherals
-

Linux Network Connectivity

- Network Configuration
 - Domain Name Systems (DNS) Configuration
-

Linux Scripting

- A Shell variables
 - If, for, while
 - Writing advanced scripts
-

Optimizing Linux Systems

- Monitoring System Resources
-

Working with Users and Groups in Linux

- Understanding Linux Users and Groups
 - Administrating Users and Groups
-

Securing Linux server

- Applying Object Permissions
 - Extending Object Usability
-

Exam Preparation

- Preparation for LPI Linux Essentials Exam

02

Networking (80 hours)

Subject	Description
Introduction to networking	Introduction to communication , types of equipment, OSI model, TCP/IP model
Layer 1	RJ45 , Cables STP/UTP , Fiber optics , RS232 , Serial , Computer architecture
Layer 2	LAN,WAN , Ethernet, MAC addresses , static/dynamic learning , unicast/broadcast/multicast, VLANs, Spanning tree
Layer 3	IPv4, Public address/Private address, Subnets, CIDR, IPv6, Decimal/Octal/Hex conversion , Network topology, Proxy , Routing (Static/Dynamic protocols)
Layer 4 - Network Protocols	HTTP , HTTPS, Telnet , SSH, DNS, DHCP, SNMP, SMTP FTP
Routing	Static and Dynamic routing (EIGRP , OSPF,BGP)
Basic configuration of Switches and routers with the CLI	Working with packet tracer , Configure VLANs, Port mirroring , Trunk/Access , Routing on stick , CLI commands, port security, Access lists , users , logins , line VTY
Final Project	CLI, Basic switch and end device configuration, console cable, Telnet & SSH (On Router)

03

System (128 Hours)

Subject	Description
Introduction to Virtual environment	VMware\Hyper-V
Introduction to Operating System	Windows 10 - Install And Configure
Workgroup \ Domain \ Troubleshoo	
Server 2016\2019	Installation Roles & Features - Tools
Active Directory Introduction	
Active Directory	Installation & Configure
Active Directory Users & Computers	Users \ Security Group \ OU Design
File Management	NTFS\Share Permissions (Shadow copy)
Registry + Group Policy	
Password Policy / Auditing Policy / Fine Grained Password Policy / Security Policy	
Securing Windows Server by Using Group Policy Objects	

Patch Management

WSUS

**Storage + Data
transition methods**

RAID Levels (openfiler) Data transitions methods + Audit

Windows Backup

**Business continuity
and DR**

BCD Methods

Cloud computing

Office 365, Azure, AWS

Material Recap

Material Recap

Final Project (System)

Hand-On Labs Project

04

Cyber Security (160 Hours)

Subject	Description
Network traffic Analyzing	Working with Wireshark, NMAP, Type of sniffers, installation, extracting credentials from network traffic, methods of extracting files and objects from network traffic. Follow sessions, and filters and statistics
Working with Python	What is programming language, open new project in pycharm, operators, basic \0 commands, if else, conditions, loops.
Introduction to KALI Linux	Installation, Linux's concept, working with the Terminal, tools etc.
Reconnaissance Methods	Google Hacking (with regex), Social Engineering
Infrastructure attacks	UDP Flood, SYN Flood, DDOS, ARP poisoning, ARP spoofing and MAC spoofing, MITM
Mitigation of Infrastructure attacks	Encryption, Digital Certificate, NAC, etc.
Password cracking and Mitigation	Cryptographic Hash functions, Brute Force, Rainbow tables, Password Hijacking
Application security - hacking and mitigation	Databases and SQL, SQL injection.CSRF, Path Traversal, XSS, Session Hijacking, Buffer Overflow, Privilege escalation
Exploits and Working with Metasploit	
From Cyber-attack to Cyber security	Concept of cyber defense vs hacking etc.

End Point security EMMET (including DEP, ASLR, SEH), HIPS, DLP, AV, app-lockers

Organization network security FW and ACL, IPS, NAC, Web Application Control, security VPN, DNS Sec, IPsec, Content Disarm and Reconstruction, Waterfalls, SIEM. Information security and risk assessment standards.

Patch management and vulnerability assessment The process of risk management and vulnerability Assessment

Forensics concepts Concept, Create HD image and mem dump, Analyzing mem dump and HD image

Audit Concepts

Static and Dynamic malware analysis Strings, exported and imported DLLs, hash, PE malware analysis structure etc. Using sandbox, Sysinternals and other basic tools

Data encryption and authentication

**Law and Ethics/
Physical Security**

Final Exam Hands-On Labs and simulator

05

Cyber AI (40 hours)

Subject	Description
LLM Fundamentals & Operational Principles for Cyber Offense	LLM Architecture & Evolution: <ul style="list-style-type: none">- Deep dive into transformer architecture, Diffusers, Generative, self attention, tokenization, Model training and model fine-tuning- Historical Overview: Getting to know about the leading LLMs (GPT, Sonnet, Llama, DeepSeek, Qwen etc.) and their evolution Industry Tool Integration: <ul style="list-style-type: none">- Exposure to development and research tools such as Copilot and Gemini, for real-world generative and research task integration, Operational Mechanics <ul style="list-style-type: none">- How LLMs process language inputs and generate outputs- Distinctive properties of generative models versus traditional AI / ML Overview of application in Cybersecurity: <ul style="list-style-type: none">- Real World events involving GenAI vectors in offensive ops, vulnerability analysis, and automated attack simulations Hands-on Labs: <ul style="list-style-type: none">- Interactive session: Experimenting with different LLM interfaces (ChatGPT, Claude, DeepSeek, Gemini, WhiteRabbitNeo, WormGPT and more!) to understand input/output behavior on restricted and unrestricted models.- Basic prompt engineering exercises: Modify prompts to understand sensitivity and context handling
Attacking LLMs – LLM Vulnerability Analysis & Exploit Techniques	LLM Vulnerabilities Explored: <ul style="list-style-type: none">- Detailed discussion on LLM-specific vulnerabilities (prompt injection, jailbreaks, and model extraction)- Comparison of these vulnerabilities with traditional software and network weaknesses

Mechanisms of Exploitation:

- Techniques attackers use to bypass guidelines and manipulate the model for unintended outputs
- Analyzing case studies, articles and recent research papers, that highlight real-world cases of exploitation on LLMs
- tools like Gemini and Copilot in testing environments to explore vulnerabilities

Security Implications:

- The impact of subtle input changes on model outputs and operational security
- Defensive measures outlined

Ethical Snapshot:

- A reminder highlighting responsible disclosure and legal boundaries

Hands-on Labs:

- Simulation lab: Craft and test adversarial prompts in a controlled environment
- Analysis exercise: Record output variations and pinpoint which input triggered the vulnerabilities

Building Offensive Tools Using LLMs

Automated Exploit Code Generation:

- Using LLMs to generate code snippets for exploiting vulnerabilities
- Using LLMs in Malware Development

Vulnerability Scanning & Tool Integration:

- Automating vulnerability scanning and reconnaissance using LLM outputs
- Best practices for Integrating LLM-generated outputs as models into offensive cybersecurity toolkits such as Metasploit for penetration testing

Risk and Mitigation in Tool Design:

- Discussion on dual-use concerns: ensuring testing remains in a controlled environment

Hands-on Labs:

- Guided coding lab: Generate exploit payloads from textual vulnerability descriptions using an LLM interface (CVE-based prompts)
 - Integration lab: Develop a small script that automates vulnerability scanning using LLM-generated code and Python
 - automation pipelines in tool-building
-

LLM-Driven Reconnaissance & Social Engineering

Automated OSINT and Intelligence Gathering:

- Techniques for using LLMs to collect and correlate data from different public sources
- Using LLMs to build tools for automate open-source intelligence (OSINT) gathering and data collection
- Enhancing traditional OSINT with LLM-driven text analysis and summarization

Social Engineering Tactics:

- How to leverage LLMs to create persuasive phishing emails, deceptive social mediaposts, websites and other social engineering artifacts
- Analysis of successful real-world red team engagements using LLM-generated content

Operational Integration:

- How these techniques feed into broader offensive strategies and red team exercises
- Differentiating between genuine and LLM-generated intelligence

Hands-on Labs:

- Phishing simulation lab: Generate and refine phishing and social engineering messages using LLM prompts
 - OSINT exercise: Use an LLM to Analyze public data (news articles, social media feeds) and extract actionable threat intelligence
 - Build a tool to automate OSINT scraping
-

Integrated Offensive Engagement & Red- Teaming and Ethical Considerations

Integrated course concepts: from LLM fundamentalsto offensive applications:

- Bringing together reconnaissance, exploit generation, and social engineering into a full-spectrum offensive operation
- Step-by-step planning from initial discovery through to exploitation and data exfiltration

Emerging Trends in Offensive AI:

- A look into the future: new tactics, evolving vulnerabilities, and adaptive offensive AI techniques
- Discussion of defensive countermeasures against LLM generated attacks and the importance of red teaming AI systems and
- **Ethical & Legal Frameworks:**
- A concise yet thorough review of ethical, legal, and risk management considerations when conducting offensive operations
- Best practices for responsible disclosure and maintaining a secure operational boundary

Hands-on Labs:

- Comprehensive scenario simulation: Work in small groups to design an end-to-end offensive operation using LLM-based tools- each group tackles a different phase (reconnaissance, exploitation, social engineering) and then shares insights
- Discussion session: Evaluate the simulation results, focusing on both offensive

Real World Practice:

- Use of Gemini, Copilot and other built-in tools, will be emphasized in the simulation phase to reflect industry adoption and to evaluate their operational contribution in real-time defensive and offensive execution.

Total Academic hours: 506

We are waiting for you!

