BATCH 2

OUTLINE OF BATCH 2

CYBERSTER

FEATURING CC | NETWORK+ | CEH

COURSE OVERVIEW

Welcome to Cyberster Batch 2: The Zero to Hero Mastery. This isn't just a basic training program; it is an elite, 12-week intensive journey designed to transform passionate beginners into industry-ready Cybersecurity Professionals.

In an era where digital threats are evolving, “basic” knowledge is no longer enough. This batch is engineered on a Hybrid Learning Model, integrating the globally recognized standards of CompTIA Network+ and the legendary EC-Council Certified Ethical Hacker (CEH v12).

Why Cyberster Batch 2?

Unlike traditional courses, Batch 2 focuses on a "Security First" mindset combined with "Red Team" execution. We bridge the gap between knowing how a network works and knowing how to break—and then secure—it professionally.

- Hybrid Curriculum: A unique blend of Infrastructure (Network+) and Offensive Security (CEH).
- Lab-Centric Learning: The majority of the course is dedicated to hands-on practicals using industry-standard tools in controlled lab environments.
- Professional Portfolio: Every weekly task is designed to be a professional write-up, helping you build a high-impact LinkedIn presence.
- Advanced Modules: Moving beyond the basics into Vulnerability Management, Active Directory Attacks, and Web Application Pentesting.

The Goal

By the end of this 3-month journey, you will not only understand the "What" and "How" of Cyber Security but will be capable of executing full-scale attack chains, identifying vulnerabilities, and providing professional-grade security solutions.

Cyberster Premium Cybersecurity Program

"Beginner to Advanced" – 12-Week Hybrid Syllabus
Curriculum Architect Design | MWF Schedule | 2 Hours/Session

PHASE 1: THE INFRASTRUCTURE SPECIALIST (Weeks 1-6)

Foundation: Network+ Architecture + Cyber Security Fundamentals

1. Enterprise Architecture & Security-First Design

- Designing resilient layouts using the industry-standard CIA Triad.
- Building and securing enterprise-grade network architectures from scratch.
- Mastering data flow mechanics and multi-vendor infrastructure communication.
- Implementing Infrastructure-as-Code principles for scalable security environments.
- Developing logical layouts to eliminate single points of failure.

2. Logical Segmentation & Traffic Control

- Implementing high-level addressing frameworks across Hybrid Cloud environments.
- Mastering Layer 2 Operations and secure traffic isolation via advanced switching.
- Deploying complex routing logic to eliminate lateral movement vulnerabilities.
- Managing traffic flow efficiency and redundant gateway operations.
- Transitioning flat networks into a modernized Zero Trust Architecture.

3. Linux Core & System Hardening

- Professional CLI mastery and virtualization architecture for security labs.
- Implementing the Principle of Least Privilege across critical system environments.
- Attack surface reduction and advanced system control techniques.
- Managing secure file systems and high-level directory permissions.
- Deploying system-level hardening to neutralize unauthorized service execution.

4. Security Automation & Scripting

- Real-time diagnostics and system health monitoring for continuous uptime.
- Developing custom Bash scripts for end-to-end security task automation.
- Identifying malware persistence and clearing hidden system traces.
- Automating routine backup cycles and critical log management systems.
- Building automated port scanners and custom IP monitoring tools.

5. Risk Governance & Infrastructure Defense

- Implementing Information Assurance pillars and robust MFA frameworks.
- Strategic Risk Management: From threat identification to professional mitigation.
- Developing Defense-in-Depth through technical and administrative controls.
- Mastering the lifecycle of risk treatment (Avoid, Mitigate, Transfer, Accept).
- Building secure infrastructure perimeters using DMZs and VPN tunnels.

6. Access Warfare & Identity Management

- Advanced Access Control Models (RBAC/MAC) and modern identity perimeters.
- Data security through industry-standard encryption and hashing protocols.
- Developing Incident Response & Business Continuity (BC/DR) foundations.
- Systematic identification of Web Exploitation basics and injection vulnerabilities.
- Implementing defensive credential strategies to prevent modern identity theft.

PHASE 2: THE ETHICAL HACKER (Weeks 7-12)

Offensive Focus: CEH Attack Methodologies + Network+ Exploitation Vectors

7. Traffic Intelligence & Core Service Mechanics

- Deep dive into **Recursive & Iterative DNS Resolution** for global communication.
- Mastering the **DORA Process** and automated dynamic host configuration.
- Implementing **Network Address Translation (NAT/PAT)** to mask internal IP architectures.
- Analyzing real-time communication performance: Latency, Jitter, and Throughput.
- Diagnostic mastery: Utilizing advanced ICMP protocols for network path discovery.
- Developing "Traffic Visibility" to identify anomalies in public vs. private data flow.

8. Advanced Infrastructure Defense & Connectivity

- Implementing **Stateful vs. Stateless Inspection** via next-gen firewalls.
- Deploying "Deny All" security postures and granular inbound/outbound rule-sets.
- Integrating **Detection vs. Prevention (IDS/IPS)** for active threat blocking.
- Mastering Site-to-Site and Remote Access **VPN Tunneling & Encryption.**
- Centralized infrastructure monitoring using **Syslog and SNMP** frameworks.
- Diagnosing complex connectivity failures using low-level CLI diagnostic suites.

9. Intelligence Gathering & Vulnerability Analysis

- The Art of Reconnaissance: Mastering Passive vs. Active information gathering.
- Advanced **OSINT (Open Source Intelligence)** techniques for digital footprinting.
- High-speed port scanning and service version detection using the **Nmap Scripting Engine.**
- Identifying, categorizing, and prioritizing security flaws in enterprise assets.
- Utilizing automated vulnerability scanners for full-scale network topology mapping.

- Developing a "Threat Blueprint" to prevent exploitation attempts before they occur.

10. Gaining Access & Tactical System Exploitation

- Mastering **Exploitation Framework architectures**: Payloads, Auxiliaries, and Post-modules.
- Delivering tactical payloads via advanced client-side engineering.
- **Password Warfare**: Executing dictionary and brute-force attacks against weak hashes.
- Connection Management: Mastering **Reverse vs. Bind Shell** listener protocols.
- Maintaining tactical access during complex network transitions.
- Understanding the "Meterpreter" workflow for high-level system control.

11. Active Directory Mastery & Post-Exploitation

- Navigating the **Corporate Backbone**: Domain Controllers, Forests, and Trees.
- Managing enterprise-wide permissions through **Group Policy Objects (GPOs)**.
- Tactical Privilege Escalation: Transitioning from standard users to Domain Admin.
- Exploiting service account misconfigurations in a live AD environment.
- Utilizing post-exploitation toolsets to identify high-value targets within a domain.
- Understanding **LDAP/DNS** roles in maintaining corporate identity perimeters.

12. Tactical Persistence & Professional Reporting

- Implementing **Persistence Mechanisms**: Backdoors, Web Shells, and Scheduled Tasks.
- Operational Security: Clearing system tracks and modifying logs to remain undetected.
- Professional **Reporting Frameworks**: Drafting Executive Summaries for C-Suite.
- Translating technical findings into "Actionable Defense" for clients.
- The Full Attack Chain: Executing and documenting **Recon → Exploit → Persist**.
- Final Capstone: Turning complex cyber attacks into professional-grade security audits.

Program Differentiators (Premium Value)

Feature: Hybrid Curriculum
Cyberster Implementation: Every concept taught through two lenses: Network+ (how it works) and CEH (how to break it). Theory and offensive execution, always together.

Feature: Lab Infrastructure
Cyberster Implementation: Structured local lab environments using free open-source tools (Kali Linux, Metasploitable, OWASP Juice Shop, VulnHub VMs) with guided setup support provided to every student

Feature: Portfolio Development
Cyberster Implementation: Weekly LinkedIn tasks build a public professional brand; final capstone report becomes portfolio centerpiece

Feature: Career Integration
Cyberster Implementation: Week 12 includes professional reporting which forms the backbone of any career in Cyber Security.

Feature: Instructor Support
Cyberster Implementation: MWF live sessions + async lab support via WhatsApp + weekly working hours for 1:1 mentoring

Prerequisites & Technical Requirements

Student Requirements:
- Basic computer literacy (file management, CLI navigation)
- 8GB RAM minimum, 50GB free storage, virtualization-enabled CPU
- Stable internet connection for cloud lab access

Pre-Program Prep (Provided):
- 3-hour "Cyber Foundations Bootcamp" video series (Linux CLI, networking basics, VM setup)
- Tool installation scripts (Kali Linux, Windows evaluation VMs, Docker)
- Legal authorization template for personal lab testing

"This syllabus doesn't just teach cybersecurity—it forges cybersecurity professionals. Every lab is a battle simulation, every concept is mapped to real-world impact, and every graduate leaves with a portfolio that proves capability, not just completion."