ECHO

Cybersecurity Fundamentals

A complete career journey designed for beginners.
Learn step by step. Practice through hands-on labs.
Build real projects. Graduate job-ready.

Echo · *Learn. Practice. Build. Launch.*

ABOUT THIS JOURNEY

Built for Complete Beginners

No previous cybersecurity knowledge is required. This roadmap is designed to take you from zero experience to becoming genuinely job-ready — step by step, skill by skill, project by project. The objective is not simply to finish a course. The objective is to become ready for the cybersecurity job market.

Beginner Friendly

No prior knowledge needed. Start from zero.

Step-by-Step Learning

Every concept builds on the last, nothing is skipped.

Hands-on Labs

Practice with real tools in controlled environments.

Mini Projects

Apply skills to real scenarios that build your portfolio.

Career Focused

Every lesson is designed with your first job in mind.

Industry Best Practices

Learn what employers actually look for and expect.

YOUR JOURNEY WITH ECHO

From Zero to Job-Ready

Echo has already built the path. You simply follow the journey.

01

Complete Beginner

No experience required — start exactly where you are.

02

Learn Security Fundamentals

Build a strong technical foundation through structured modules.

03

Practice Weekly Labs

Reinforce every concept with guided, hands-on practice.

04

Build Mini Projects

Apply what you learn to real-world scenarios.

05

Create GitHub Portfolio

Showcase your work professionally to future employers.

06

Optimize LinkedIn & CV

Build an ATS-friendly CV and a powerful LinkedIn presence.

07

Interview Preparation

Master technical and behavioral interview skills with mentorship.

08

First Cybersecurity Job

Land your first opportunity with Echo's ongoing support.

> We don't stop when the course ends. We continue until you're ready for your first opportunity.

PHASE 1

Security Foundations

Begin your cybersecurity career with the knowledge every professional relies on. You'll understand how threats work, how organizations defend against them, and how the industry thinks about risk, trust, and protection.

Key Topics

Core Concepts

- Information Security & Cybersecurity Frameworks
- CIA Triad · Access Control · Security Controls
- Blue Team vs Red Team · Threat Actors
- Attack Surfaces · Social Engineering

Cryptography

- Symmetric & Asymmetric Encryption
- Hashing · Encoding · Compression
- Digital Signatures

Hands-on Lab & Mini Project

Mini Project

Analyze a phishing scenario and identify security controls that could prevent the attack.

Skills You'll Gain

- Security mindset and threat awareness
- Understanding of encryption and data protection
- Foundation for all advanced cybersecurity topics

Career Benefit

Every cybersecurity role — from analyst to penetration tester — requires this knowledge as a baseline.

PHASE 2

Networking

Networks are the backbone of every digital environment. Mastering networking is essential to understanding how attacks travel, how traffic is analyzed, and how defenses are architected.

Key Topics

Network Fundamentals

- OSI Model · TCP/IP · IPv4 · Subnetting
- Routing & Switching · TCP · UDP · ICMP
- ARP · DHCP · DNS · SMB
- SMTP · SNMP · Firewalls · Proxies

Traffic Analysis

- Wireshark — packet capture & inspection
- Protocol identification & anomaly detection

Hands-on Lab & Mini Project

Mini Project

Build and analyze a small network using Packet Tracer and inspect live traffic with Wireshark.

Skills You'll Gain

- Deep understanding of how data flows across networks
- Ability to read and analyze network traffic
- Foundation for network attacks and defense

Career Benefit

Network knowledge is tested in virtually every cybersecurity interview and used daily by security analysts.

PHASE 3

Linux Fundamentals

Linux powers the majority of servers, cloud environments, and security tools. You'll master the command line and gain the confidence to operate in real professional environments.

Key Topics

Core Skills

- Linux Distributions · File System · Navigation
- Users · Groups · Permissions
- Processes · Pipes · Redirection
- Base64 · Hex · INodes · Symbolic Links
- Run Levels · Logs · Networking

Mini Project

Secure a Linux system: create users, configure permissions, and analyze log files.

PHASE 4

Windows Fundamentals

Windows dominates enterprise environments. You'll learn to navigate, administer, and secure Windows systems — including Active Directory, the backbone of corporate IT.

Key Topics

Core Skills

- Windows Basics · Registry · File System
- Event Logs · Permissions · Networking
- Windows Server · Active Directory
- PowerShell scripting and automation

Mini Project

Deploy a Windows Server, create Active Directory users, and configure Group Policies.

PHASE 5

Reconnaissance & Vulnerability Assessment

Learn to think like an attacker. You'll use professional tools to gather intelligence, enumerate targets, and identify weaknesses — then document your findings in a professional report.

Key Topics

- Passive Recon: WHOIS · Shodan · Google Dorking
- Active Recon: Port Scanning · DNS Enumeration
- Nikto · Directory Enumeration · Banner Grabbing
- Vulnerability Scanners · Misconfigurations

Mini Project

Perform full reconnaissance against a lab environment and produce a professional assessment report.

PHASE 6

Network Attacks

Understand how attackers exploit networks at a technical level. You'll capture and analyze traffic, identify attack patterns, and build the awareness needed to detect and respond to threats.

Key Topics

- Authentication · Password Security
- Windows Shares · Null Sessions
- ARP Poisoning · FTP · SMTP · SNMP
- Traffic Analysis with Wireshark

Mini Project

Capture network traffic using Wireshark and identify suspicious communication patterns.

PHASE 7

System Attacks & Security Awareness

Explore how attackers target operating systems, escalate privileges, and deploy malware — then learn how defenders detect, investigate, and respond to these threats.

Key Topics

Password Attacks

Brute force, credential stuffing, and dictionary attacks

Active Directory Attacks

Core AD attack concepts and lateral movement awareness

Malware Fundamentals

Types, behaviors, delivery methods, and evasion techniques

Indicators of Compromise

IOCs and basic malware analysis concepts

Mini Project

Controlled Malware Analysis

Analyze malware behavior inside a controlled lab environment and identify Indicators of Compromise. Document your findings in a professional security report.

Skills You'll Gain

- Offensive awareness to strengthen defensive decisions
- Ability to analyze and document malware behavior
- SOC analyst-ready incident investigation skills

Career Benefit

System attack knowledge is essential for SOC analysts, incident responders, and penetration testers alike.

BEYOND LEARNING

Echo Builds Your Career, Not Just Your Skills

Technical knowledge is only one part of landing your first role. Echo provides the complete professional infrastructure you need to be seen, selected, and hired.

Professional GitHub Portfolio

Showcase labs and mini projects that prove your hands-on capabilities to employers.

LinkedIn Optimization

Build a professional LinkedIn profile that attracts recruiters in cybersecurity.

ATS-Friendly CV Creation

A professionally structured CV designed to pass applicant tracking systems.

Interview Preparation

Technical and behavioral interview coaching with real practice questions.

Career Mentorship

Personalized guidance from professionals who have been where you're going.

Internship & Job Application Support

Guidance on applying, networking, and securing your first cybersecurity opportunity.

Your Career Starts Here.

Learning cybersecurity is only the beginning.
Our mission is helping you build the skills, confidence, portfolio, and professional profile needed to launch your first cybersecurity career.
Echo will support you from your very first lesson until you're ready to take your first step into the industry.

Learn	**Practice**
Build	**Get Hired**

Echo · *Learn. Practice. Build. Launch.*