Full-Stack Cybersecurity Specialization Program

Duration: 12 Weeks | **Total Hours:** 72, **Schedule:** 3 Days/Week | 2 Hours/Day

---

Learning Outcomes

By completion, students will be able to:

- Understand end-to-end cybersecurity fundamentals
- Perform ethical hacking and exploit vulnerabilities safely
- Analyze, detect, and mitigate threats
- Use Kali Linux for real-world assessment
- Build secure systems in modern infrastructures
- Conduct incident investigations and response plans

Week 1: Cybersecurity Foundations

Goal: Build a solid base in core cybersecurity principles and networking.

Day	Topic	Theory	Practical
1	Introduction to Cybersecurity	Security concepts; CIA Triad; Threat Landscape	Kali Linux basics: Update, users, shells
2	Networking Fundamentals	TCP/IP, OSI, ports, subnets	Wireshark basics: Capture & analyze packets
3	Cybersecurity Workflow	Risk, Vulnerability, Threat	Lab: Identify attack surfaces in simple network

---

Week 2: Linux & Command Line Security

Goal: Hands-on mastery of Linux environment (Kali Linux).

Day	Topic	Theory	Practical
1	Linux Security Basics	File permissions, users, groups	Kali Lab: chmod, chown, sudo
2	File Systems & Logs	Syslog, audit logs	Logging with rsyslog, journalctl
3	Bash Scripting	Automation fundamentals	Write scripts to automate reconnaissance

---

Edversity.

Week 3: Reconnaissance & Scanning

Goal: Learn how attackers map and scan networks.

Day	Topic	Theory	Practical
1	Reconnaissance Overview	OSINT, information gathering	OSINT tools: Maltego, theHarvester
2	Port & Vulnerability Scanning	Nmap, TCP/UDP scan types	Nmap lab: Scan target networks
3	Service Enumeration	Banner grabbing, versions	Nikto, Dirb, enum4linux

---

Week 4: Web Security Fundamentals

Goal: Understand common web app vulnerabilities + exploitation.

Day	Topic	Theory	Practical
1	Web Architecture	HTTP/S, cookies, sessions	Burp Suite intro: Intercept traffic
2	OWASP Top 10	SQLi, XSS, CSRF, etc	Lab: Exploit OWASP Juice Shop
3	Input Validation	Sanitization, filtering	Practice SQLi & XSS on DVWA

Week 5: Exploitation & Post-Exploitation

Goal: Learn exploitation basics and control over compromised hosts.

Day	Topic	Theory	Practical
1	Metasploit Framework	Concepts, modules, payloads	Build exploits with msfconsole
2	Shells & Persistence	Reverse shells, backdoors	Create and execute payloads
3	Privilege Escalation	Linux & Windows	Post-exploit enumeration & escalation

---

Week 6: Industrial Workshops and Assessments

Goal: Equip students with Industrial knowledge and evaluations.

Day	Topic	Theory	Practical
1	Mid-Project Assessments, Practice Sessions, and Industry Workshops		
2			
3			

Edversity.

Week 7 & 8: Defensive Security & Incident Response

Goal: Shift focus to defense, detection, incident handling.

Day	Topic	Theory	Practical
1	Security Monitoring	SIEM, IDS/IPS	Snort / Suricata basics
2	Incident Response Procedures	Playbooks, triage	Simulate incident response workflow
3	Secure Log Management	Centralization, analysis	ELK Stack basics for log analysis

---

Week 9 & 10: Cloud & Modern Infrastructure Security

Goal: Explore cloud security, DevSecOps, and containers.

Day	Topic	Theory	Practical
1	Cloud Security Essentials	Shared responsibility model	AWS IAM & Security Groups demo
2	Containers & Kubernetes Security	Microservices risks	Scan Docker images for vulnerabilities
3	DevSecOps	CICD pipelines, toolchain	Secure pipeline lab (GitHub + SAST)

Week 11: Advanced Topics & Capstone

Goal: Integrate concepts into real-world scenarios + assessments.

Day	Topic	Theory	Practical
1	Zero Trust & Modern Defense	Identity security	Configure network segmentation
2	Capstone Project	Understanding and project Development	Students will prepare a project related to their understanding.
3	Final Assessment	Scenario-based evaluation	Full-scale attack/defense lab

---

Week 12: Assessments and Projects

Goal: Equip students with Industrial knowledge and evaluations.

Day	Topic	Theory	Practical
1	Final-Project Presentations, Practice Sessions, and Industry Workshops		
2			
3			

Tools Covered

Domain	Tools
Reconnaissance	theHarvester, Maltego
Scanning	Nmap, Nikto, Dirb
Vulnerability	OpenVAS, Nessus
Exploitation	Metasploit, Burp Suite
Network Monitoring	Wireshark, Snort
Logging / SIEM	ELK, Splunk (demo)
Cloud	AWS IAM, Security Groups

Assessment & Certification

- Weekly quizzes & participation
- Midterm practical evaluation (Week 6)
- Final capstone exam & CTF-style challenge
- Certificate on completion