ACE IT CAREERS
BEST CAREER BUILDER

CYBERSECURITY · COURSE SYLLABUS

Cybersecurity Analyst Training

A practical, tool-based cybersecurity program covering system hardening, network and vulnerability assessment, web application and cloud security, penetration testing and professional security reporting.

8 Weeks | Live online | Placement support

Syllabus

WEEK 1

Foundations of system security

- System security baselines
- Hardening techniques
- Patch management strategies

Tools: CIS-CAT, Lynis, OpenSCAP, Ansible

WEEK 2

Network vulnerability analysis

- Port scanning
- Service enumeration
- Wireless network assessment

Tools: Nmap, Masscan, Netcat, Wireshark

WEEK 3

Vulnerability assessment

- Enterprise vulnerability scanning
- Report generation for security teams

Tools: Nessus, OpenVAS, Qualys, Dradis

WEEK 4

Web application security basics

- HTTP/HTTPS traffic analysis
- Finding server misconfigurations

Tools: Burp Suite, OWASP ZAP, DVWA

WEEK 5

Advanced web application security

- Authentication testing
- Cross-site scripting (XSS)
- SQL injection (SQLi)
- Fuzzing and advanced payloads

Tools: SQLMap, wfuzz, Burp Suite Pro

WEEK 6

Cloud security assessment

- Cloud infrastructure security
- Container security for Docker and Kubernetes
- Serverless environment evaluation

Tools: AWS Inspector, Docker Bench, kube-bench

WEEK 7

Penetration testing and offensive security

- Simulating real-world attacks in a lab
- Evaluating defensive controls and breach exposure

Tools: Kali Linux, Metasploit, Empire

WEEK 8

Capstone and integration

- Full-scope security assessment
- End-to-end security report

Tools: All tools from previous weeks, Dradis for final reporting

Included with every course

- Live instructor-led classes in US time zones, with session recordings
- Real-time project work and a certificate
- Resume preparation and marketing, mock interviews and placement support