

Cybersecurity & Ethical Hacking Foundations

Learn networking, Linux, security fundamentals and vulnerability assessment — legally, ethically and only in authorised labs

Cybersecurity · beginner · Live online, instructor-led

This syllabus is a draft awaiting instructor review and may change.

A twelve-week live course in security foundations: networking, Linux, cryptography, threat modelling, web application security and vulnerability assessment. All hands-on work happens in authorised lab environments, never on real third-party systems.

Length and schedule

48 hours of live teaching, on either schedule:

- Weekday Intensive (Mon–Fri): about 10 weeks before holidays
- Weekend Evening (Sat & Sun evenings): about 12 weeks before holidays

Fees per student, whole course

- Group: Rs. 14,999
- Duo: Rs. 24,999
- One-to-One: Rs. 44,999

Launch fee — GST treatment to be confirmed.

What you will be able to do

- Explain the ethical and legal limits of security testing, including the IT Act, 2000 at an overview level, and work only within an authorised scope
- Build and use an isolated virtual lab for safe practice
- Describe how networks work and analyse traffic with Wireshark in the lab
- Administer a Linux system from the command line and write simple Bash scripts
- Apply core security concepts: the CIA triad, cryptography, authentication and access control
- Threat-model a simple application and propose controls for the risks you find
- Identify and explain common web vulnerabilities from the OWASP Top 10 in deliberately vulnerable lab applications
- Run a scoped vulnerability assessment in the lab, rate findings with CVSS and write a clear report with remediation advice
- Follow responsible disclosure practice when reporting a vulnerability

Before you start

- Comfortable using a computer, installing software and working with files and folders
- No previous security, networking or Linux experience required; basic programming is helpful but not needed
- A laptop that can run two or three virtual machines at once: 8 GB RAM minimum, 16 GB recommended, about 80 GB of free disk space and hardware virtualisation enabled
- Agreement to the course rules: all testing only on systems you own or have written permission to test, inside the provided lab environments

Tools

VirtualBox or VMware Workstation Player, Kali Linux, Ubuntu Linux, Wireshark, Nmap, Burp Suite Community Edition, ZAP, OWASP Juice Shop and DVWA (deliberately vulnerable practice applications), Greenbone Community Edition (OpenVAS), OWASP Threat Dragon

Syllabus

Module 1: Security foundations, ethics and the law

What cybersecurity covers, the legal and ethical limits of testing, and a safe lab to practise in.

1. What cybersecurity is (2 h)
2. Ethics, authorisation and Indian law (2 h)
3. Building the lab and doubt-clearing (2 h)

Module 2: Networking for security

How data moves across networks, and how to see it.

4. How networks work (2 h)
5. IP addressing, subnets and ports (2 h)
6. Core protocols: DNS, HTTP and TLS (2 h)
7. Packet analysis lab and doubt-clearing (2 h)

Module 3: Linux and the command line

Run and inspect Linux systems confidently, the way security work requires.

8. Linux fundamentals (2 h)
9. Users, permissions, processes and logs (2 h)
10. Bash scripting and doubt-clearing (2 h)

Module 4: Security fundamentals and threat modelling

The building blocks of protection, and a structured way to find risks before attackers do.

11. Cryptography in practice (2 h)
12. Identity, authentication and access control (2 h)
13. Threat modelling (2 h)
14. Defensive controls, incident response and mid-course review (2 h)

Module 5: Web application security

How web applications are attacked and defended, practised only on deliberately vulnerable lab applications.

15. How web applications work and the OWASP Top 10 (2 h)
16. Injection flaws (2 h)
17. Cross-site scripting, CSRF and broken access control (2 h)
18. Web security lab and doubt-clearing (2 h)

Module 6: Vulnerability assessment and responsible disclosure

Run a structured, authorised assessment from scope to report, and report issues the responsible way.

19. Assessment methodology, scope and reconnaissance (2 h)
20. Scanning and enumeration (2 h)
21. Validating findings and rating risk (2 h)
22. Reporting, responsible disclosure and doubt-clearing (2 h)

Module 7: Capstone assessment

Bring everything together in a scoped lab assessment and present the results.

- 23. Capstone lab studio and doubt-clearing (2 h)
- 24. Capstone presentations and final assessment (2 h)

Final project

Assess a deliberately vulnerable lab application and network, and write a professional report. You receive a written scope and rules of engagement for a target environment that runs only inside the course lab. Nothing outside that scope may be touched. You will:- produce a short threat model of the target application with a data-flow diagram and the main risks;- perform reconnaissance and scanning of the in-scope lab hosts only, keeping a timestamped activity log;- identify and safely validate at least five vulnerabilities, including at least two in the web application;- rate each finding with CVSS and explain its business impact in plain language;- recommend specific, prioritised fixes and explain how to verify each one;- write a responsible-disclosure note describing how you would report one finding to a real vendor. Deliverables: the activity log, the threat model and a written assessment report (executive summary, scope, methodology, findings, remediation) presented live in the final week. Testing anything outside the provided scope fails the project.

Certificate

- At least 80% attendance
- All assignments submitted
- Projects passed
- Final assessment passed (60%)

A ZORK Academy course completion certificate; paying for the course does not by itself earn it.

Next step

Book a free consultation: <https://zorkacademy.online/consultation?course=cybersecurity-ethical-hacking>

We help you prepare for work; we do not guarantee jobs, placements or salaries.