

Cybersecurity: Career Paths, Skills & Opportunities – Protect the Digital World

Cybersecurity is a dynamic and growing field offering diverse opportunities for students interested in protecting digital assets.

Samrachana Baral





What is Cybersecurity?

Protecting systems, networks, and data from digital attacks



Confidentiality, Integrity, Availability – core principles
that secure information

Protects systems, networks, and data **from digital attacks**

Key threats: **ransomware**, data breaches, financial theft,
privacy violations

Understanding fundamentals helps students grasp why security
measures are vital today

Why Cybersecurity Matters Now

Threats rising in frequency and sophistication driven by AI

Rapid cloud adoption increases attack surface and new vulnerabilities

Organizations need skilled cybersecurity professionals to defend assets

Career opportunity: growing demand as threats and cloud use expand

Cybersecurity in the IT Ecosystem

Developers – Secure Coding

Embed input validation, secrets handling, and secure libraries into code.

DevOps – DevSecOps Pipelines

Automate security checks in CI/CD: SAST, DAST, dependency scans.

Management – GRC (Governance, Risk, Compliance)

Set policies, manage risk assessments, and ensure regulatory compliance.



Data & AI – Privacy & Secure ML Protect data, apply privacy controls and defend ML models from attacks.

Cloud Engineers – Cloud Security

Configure secure cloud networks, IAM, encryption, and monitoring.

Cybersecurity Career Paths

Clear pathways for technical and non-technical roles in security

Technical roles

- **Security Analyst** — monitor threats and alerts and perform log analysis across environments.
- **Penetration Tester** — conduct ethical hacking to discover vulnerabilities and validate defenses.
- **Incident Responder** — triage incidents, contain threats, and coordinate remediation.
- **Security Engineer / Cloud Security Engineer** — design and build secure systems, automate controls, and harden cloud infrastructure.

Non-technical & semi- technical roles

- **GRC Analyst** — governance, risk & compliance: policy, audit readiness, and control mapping.
- **Risk Management** — assess enterprise risk, prioritize mitigations, and advise stakeholders.
- **IAM Specialist** — design and manage identity and access controls, provisioning and policies.



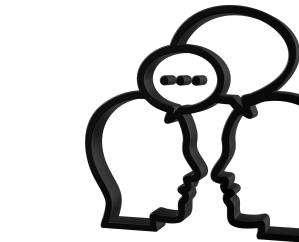
What Skills Do You Need?

Technical foundations plus soft skills for effective investigations and collaboration



Technical skills

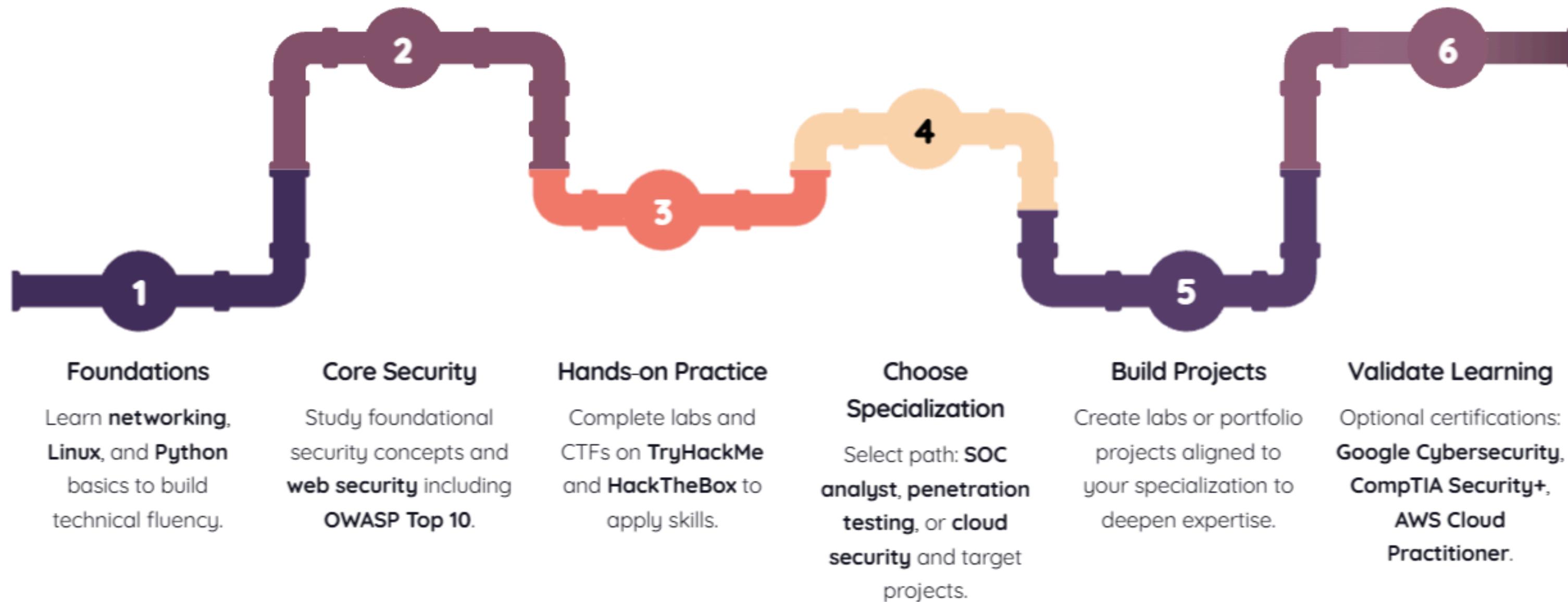
- Networking fundamentals (TCP/IP, routing, ports, protocols)
- Linux command proficiency and shell use
- Python scripting for automation and analysis
- SIEM tools, OWASP Top 10 awareness, and cloud basics



Soft Skills

- Analytical thinking for root-cause investigations
- Problem solving under pressure
- Clear documentation of findings
- Effective communication and collaboration

Beginner Roadmap



Tools You Should Know

Key cybersecurity tools and the concepts to learn from each

Wireshark – network packet analysis; learn traffic patterns and protocols

Nmap – host and port scanning; learn discovery, fingerprinting, and timing

Burp Suite – web app testing; learn request/response manipulation and proxy workflows

Metasploit – exploitation framework; learn payloads, modules, and post-exploitation concepts

Splunk / Wazuh – log management; learn indexing, search, and alerting strategies

OWASP Juice Shop – practice platform; learn common web vulnerabilities hands-on

Kali Linux – pentesting environment; learn toolchains, scripting, and OS-level workflows

Focus on concepts over mechanics – why tools work and attack/defense principles

Common Myths vs. Reality

Debunking barriers that stop beginners from entering cybersecurity

Myths

- Only like 'hacking movies'
- Requires expert coding skills
- No entry-level opportunities

Facts

- Many roles focus on systems, policy, and analysis
- Several paths need limited coding; tools and frameworks help
- Beginner-friendly jobs and training pathways exist

Q/A



