

Cybersecurity & Ethical Hacking

Duration	Live classes	Schedule	Batch size
12 weeks	120 hours	Mon to Fri, 2 hrs/day	10 students max

Tools you will use

- Kali Linux
- Burp Suite
- Nmap + Wireshark
- Metasploit
- nuclei + httpx
- OWASP Top 10

10 students a batch. Exceptional mentors who guide you personally, and a **syllabus built from real job posts**, cuz we never skip the "hard parts" 😊

The class

10 per batch

Ten students. Never more.

A hard cap, not a target. Your mentor knows your name and your work.

The mentor

4–5 yrs in the job

Someone who does the job.

Working professionals, not full-time teachers. They read your work line by line.

The syllabus

1/3 is fundamentals

The hard parts, not just the basics.

Teaches everything the job needs and never skips the hard parts most courses skip, built from real job descriptions. Check the syllabus before you enroll.

Built into every course

- Gate assessment**
A short test before Day 1 finds your strengths and pace, then sets your plan.
- Revision every 5th class**
Every fifth class goes back over the week, so nothing piles up.
- Certification exam**
Pass the exam at the end of the course to earn your certificate.
- A real, live project**
Every course ends with a deployed project you can show employers.
- 1:1 mock interview**
A real interview practice with your mentor in the final week.
- CV and LinkedIn help**
We help you rewrite your CV and LinkedIn before you apply.

Cybersecurity & Ethical Hacking

Why This Course

You train for two junior jobs that employers hire for: web and API VAPT analyst, and Tier-1 SOC analyst. VAPT means finding and proving security holes in a system, with written permission. A SOC is the team that watches a company's security alerts.

- **You learn the basics before any hacking.** Weeks 1 to 4 cover networks, information gathering (recon) and Linux.
- **You spend 4 weeks testing websites and APIs.** An API is the hidden connection apps use to send data. This part ends with a VAPT report you can show employers.
- **You prepare for real security certificates.** You take eJPT practice quizzes in Weeks 3, 5, 9 and 12. They lead toward Security+, eJPT, CEH and OSCP.
- **You also learn the defending side.** In Week 10 you read Active Directory logs, build a home SIEM and work a practice SOC shift. A SIEM is a tool that collects security logs in one place.
- **You use AI, but you still decide.** AI helps you draft reports and find recon ideas. Your own judgment makes the final call.

Pay depends on your skills, portfolio and clients. We do not promise a salary.

Who Is This Course For

- **Complete beginners** who use a computer well and want a real path into junior pen-testing (attacking systems, with permission, to find weak spots).
- **IT, networking or support staff** who want to move into security.
- **CS or IT students** aiming for junior pen-test or SOC analyst jobs.
- **Developers** who want to build safer apps by learning how attackers break them.
- **Career changers** interested in VAPT consulting, bug bounty or freelance pen-testing. In bug bounty, companies pay you for finding security bugs.
- **Learners who want a strong base** before moving into cloud security and DevSecOps.

Course Snapshot

PARAMETER	DETAILS
Course Code	TR-04
Duration	12 Weeks (3 Months)

PARAMETER	DETAILS
Schedule	Monday to Friday, 2 Hours/Day
Total Hours	120 Hours
Batch Size	Maximum 10 Students
Course Fee	NPR 36,750
Level	Beginner → Junior Web/API VAPT Analyst
Outcome	Junior Web/API VAPT Analyst / Tier-1 SOC Analyst

Prerequisites

- You should be comfortable using a computer every day. You do not need any security background.
- You need a laptop with at least 8GB RAM and 50GB free disk space for the practice machines.
- You need a free **Obsidian** or **Notion** account for your notes. We set it up together in the Week 1 class.
- Week 1 starts from how the internet works and how attackers think, so we assume nothing.
- You take the Saarathi Gate Assessment before Day 1. It only shows where you are starting, with no pass or fail.
- You install nothing beforehand. We install VirtualBox and Kali Linux in the first class.
- If you want a head start, try the free TryHackMe Pre-Security path.
- For self-study you use the free TryHackMe and HackTheBox plans. Paid plans are optional, and you never need them to pass.

Assessments at a glance

- **Gate Assessment:** You take it before Day 1. It shows your learning style and pace, and there is no pass or fail.
- **Certification Exam:** It comes at the end of the course. It lasts 2 hours and has about 30 questions on this course. Question types include single choice, multiple choice, true or false, numbers, ordering, matching, fill in the blank, short or long answers, code where needed, and short case studies.
- **Pass mark:** You need 70 percent. You must pass to get the Saarathi Certificate of Completion.

- **Exam rules:** The exam is watched (proctored) and runs in fullscreen. Switching tabs or apps and pasting are recorded, and three strikes end the exam.
- **Question order:** You can answer in any order and go back to any question. Every question needs an answer before you submit.
- **Recommendation letters:** We give these at our choice, only to learners who pass. They are never guaranteed.

Projects

Your mentor gives you 2 projects during the course. They need to be approved before you get your certificate and before the Career Launchpad opens.

Your Learning Week

DAY	ACTIVITY
Mon–Fri	2-hour live class with your mentor, hands-on and built around projects
Mon–Fri	2 hours of self-study at home: projects, practice and fixing errors
Sunday	Open classroom. Come in to build in a quiet space, or rest.
Day 5 (every week)	In the last hour of the 2-hour class, you revise the week, practise report writing and clear your doubts

Most real progress happens between classes, when you build, break things and fix them.

Week-by-Week Curriculum

Phase 1 • Security Mindset, Networking, Recon & Host Foundations (Weeks 1–4, 40 Hours)

WEEK	FOCUS AREA	TOPICS
Week 1	Security Mindset, Authorization & Lab Discipline	- What cybersecurity actually is: the CIA triad (confidentiality, integrity, availability: data secret, unaltered, reachable) - How the internet works and TCP/IP basics: the browser (client) sends requests to servers and reads responses, over the shared rule-set computers talk on, through common ports (numbered doors, like 80 and 443) and protocols (the language behind each door)

WEEK	FOCUS AREA	TOPICS
		- Scope, authorization, ethical testing rules: the written permission that defines exactly what you may test, and the lines you never cross - Wireshark intro (records network traffic) and your first packet capture (a saved traffic recording) - Engagement vault and note discipline: one Obsidian vault (local markdown files, works offline, yours forever) or Notion workspace set up in class on Day 1, with a note template per target, every command, screenshot and finding timestamped and written down as you work; mandatory from Day 1, checked at the Week 6 1:1, and the capstone report is written out of it - Social engineering awareness: attacks that trick people instead of machines: phishing (fake emails), pretexting (cover stories), vishing (scam calls) and physical security tricks (tailgating: slipping through secure doors, badge cloning: copying access cards); why human vectors appear in pen-test scope - AI for pen-testing: ChatGPT for recon idea generation and attack-surface brainstorming (every door an attacker could try)
Week 2	Network Services & Traffic Analysis	- How networks move and control traffic: routing (the path packets take), NAT (many devices, one public address), segmentation (isolated network zones) and firewall logic (what gets blocked) - Keeping connections safe: TLS (the browser-padlock encryption), certificates (digital ID cards for sites), SSH (encrypted remote login for admins) and secure service exposure (only open what must be open) - Wireshark deeper: streams (one reassembled conversation), filters (only the traffic you care about) and protocol analysis - ARP/DNS manipulation awareness and MITM concepts: attackers lie to the address-lookup layers (ARP and DNS) to sit in the middle of traffic (man-in-the-middle) - Defensive baselining and anomaly detection: record normal traffic so anything unusual stands out
Week 3	Nmap, Enumeration & Secure Architecture	- Nmap, the standard port scanner: scan types, service detection (what software answers each open port) and safer defaults that avoid knocking over live systems - Enumeration workflow: methodically listing everything a target exposes, banner grabbing (reading announced version

WEEK	FOCUS AREA	TOPICS
		text), with httpx and subfinder from the ProjectDiscovery toolkit for probing which hosts are live and expanding in-scope subdomains - Correlating Nmap and Wireshark findings: cross-check the scanner against the raw traffic - Secure architecture: least privilege (only the access each account needs) and defense-in-depth (layered protections) - Attack-surface mapping and reduction: list every exposed service, recommend what to close - OSINT techniques (open-source intelligence, profiling a target from public information) and passive recon discipline: Google dorks (search operators for exposed files and login pages), Shodan (internet-exposed devices and services), theHarvester (email and subdomain harvesting), Maltego awareness (link-analysis graphs), building an OSINT target profile before active scanning, and never touching a target until permission is signed - Scripting strand: wrap the Nmap workflow in a Bash script (a program of terminal commands) that parses output into a service-inventory CSV (spreadsheet-friendly) - Graded eJPT prep quiz 1 (Assessment Methodologies, the information-gathering domain)
Week 4	Linux & Host Fundamentals	- Linux file system, users, groups, permissions: how a host is laid out (/etc , /var , /home) and how Linux decides who may read, change or run each file - Processes, services, startup, packages: what is running, what launches automatically, what is installed and where it came from - The terminal and shell basics: navigating, piping and reading man pages in Bash, the daily fluency every later lab assumes - SSH and firewall basics: lock remote login to keys instead of passwords, and set the host firewall to block everything inbound by default with ufw - Sudo (the run-as-admin command), shell history (your typed commands) and ops-sec habits (never leak your own secrets) - Guided privilege-escalation lab to root (limited account to full control): see how a SUID binary (runs with its owner's power, abused via GTFOBins, the public trick catalogue), a sudo misconfiguration and a cron/PATH hijack each hand over the box, then write the fix, so you understand the host before you attack one

WEEK	FOCUS AREA	TOPICS
		- Windows and Active Directory get a full blue-team block of their own in Week 10, so this week stays entirely on Linux

Phase 2 · Host Review & Web VAPT Core (Weeks 5–7, 30 Hours)

WEEK	FOCUS AREA	TOPICS
Week 5	Logging, Auditing & Host Review	- Reading what a Linux machine remembers: journald (the system journal), auth logs (who logged in when) and system messages - auditd basics: the Linux watchdog recording who touched sensitive files - Cron and systemd timers: job schedulers attackers abuse to keep access, and the persistence indicators that give them away - File integrity: take a <code>sha256sum</code> baseline before, compare after, and catch a swapped system binary (AIDE and tripwire are the packaged version of the same idea) - Log-based investigation: reconstruct what happened on a host from logs alone - Scripting strand: Bash log-triage pipeline (<code>grep/awk/sort</code>) over <code>auth.log</code> to pull failed logins and sudo events - Remediation notes from host evidence: turn log findings into fixes a sysadmin can apply - SIEM and the Tier-1 SOC on-ramp: the same logs centralised across every host (Splunk, Microsoft Sentinel, ELK), one guided search run on a sample dataset, and the triage question a SOC analyst answers all day: is this alert real, and who gets it; taught here, next to the logs it is built from - A graded SOC alert-triage practicum: ten pre-built alerts, some real and some noise, each worked into a real-or-false-positive call and an escalation note, checked against a model answer key - Graded eJPT prep quiz 2 (Host and Network Auditing)
Week 6	Web App Anatomy, Burp & Injection Fundamentals	- How a web application is built, before you attack one: HTML, CSS and JavaScript in the browser, a backend in PHP, Python, Node.js or Java with the frameworks around them (WordPress, Laravel, Django, Express, Spring), a database behind that (MySQL, PostgreSQL, MongoDB), and Apache or Nginx plus hosting in front; one request traced through every

WEEK	FOCUS AREA	TOPICS
		layer, and the bug class each layer owns - How the web talks: HTTP methods (request verbs like GET and POST), headers, cookies and sessions (how a site remembers you), plus reading a target from the client side in browser devtools and fingerprinting its stack - Burp Suite, the web tester's workbench: proxy (intercept browser traffic), repeater (resend edited requests), intruder (automated payload testing), decoder - OWASP methodology: testing to the industry playbook, mapping findings to OWASP Top 10:2025 categories (the finalised January 2026 list of common web vulnerability classes) - SQL injection (sneaking database commands through inputs), under A05 Injection, validated hands-on on PortSwigger Labs (free, legal targets) - XSS (cross-site scripting, your script in someone else's page): reflected, stored and DOM variants, also under A05 Injection - Evidence capture and findings: exact proof for every issue you find, filed in your vault; ChatGPT may draft the first wording and explain a CVSS score, you rewrite the impact line by hand - Mid-course 1:1 mentor review: a private half hour at the exact midpoint, your vault and lab work read line by line, an honest read on where you stand, and two or three things to fix in the second half, written down and closed out in Week 12; mandatory, not graded
Week 7	Auth, Access Control & Misconfiguration	- Attacking how sites prove who you are: authentication flows, password reset and MFA (multi-factor authentication, like an OTP code) - IDOR (insecure direct object reference, swapping an ID to reach someone else's data), privilege boundaries and access control (who is allowed to do what); maps to OWASP A01 Broken Access Control, still #1 in 2025 - Session management, CSRF (cross-site request forgery, tricking a logged-in browser into acting for the attacker) and token handling - Security headers (protective settings sent to the browser), unsafe uploads and default misconfigs (OWASP A02 Security Misconfiguration, #2 in the 2025 Top 10) - New 2025 categories on a target: A03 Software Supply

WEEK	FOCUS AREA	TOPICS
		Chain Failures (known-vulnerable components, dependency provenance) and A10 Mishandling of Exceptional Conditions (errors that fail open or leak), identification and reporting only - XXE (XML External Entity, an XML parser tricked into reading server files, under A05 Injection) and insecure deserialization (untrusted saved objects rebuilt into running code, under A08 Software or Data Integrity Failures): recognise and report each once on a lab endpoint, since junior job posts still name them - Capstone target selection + scope planning: pick your final-project target and agree in writing exactly what you will test

Phase 3 · API VAPT & Exploitation Toolchain (Weeks 8–9, 20 Hours)

WEEK	FOCUS AREA	TOPICS
Week 8	API VAPT & Modern Web Testing	- REST API testing (the behind-the-scenes data doors apps run on): JWT review (signed tokens proving login) and rate limits (caps on endpoint hits) - API enumeration and OpenAPI/Swagger analysis: reading an API's machine-readable docs to list every endpoint worth testing - GraphQL awareness (query-style API standard), SSRF (server-side request forgery, making the server fetch internal URLs, now reported under OWASP A01 in the 2025 Top 10) and WebSocket basics (always-open two-way connections) - Scripting strand: short Python requests script (the standard web-call library) for endpoint probing and JWT replay - Assessment methodology and proof capture: reproducer steps (exact bug-triggering commands), impact statement, CVSS justification - Drafting findings with impact and remediation - AI for pen-testing: ChatGPT for report drafting, executive summaries (the one-page manager version), plain-language remediation advice developers act on
Week 9	Network Service Attacks & the Exploitation Toolchain	- The scanning stack a working tester reaches for first: httpx to probe live hosts, nuclei run over the survivors with community templates by severity and tag, a full authenticated OpenVAS/Greenbone sweep alongside it, older scanners like Nikto read as one noisy input among several, and every result

WEEK	FOCUS AREA	TOPICS
		cross-checked (scanner plus manual reproduction plus Burp) before it counts as a finding; wireless attack theory is awareness only - Network service attacks on what you enumerated back in Week 3: SMB null sessions, FTP anonymous access, SSH user enumeration and weak-credential spray, each proven and written into a per-service playbook cross-checked against HackTricks (hacktricks.wiki) - Metasploit framework, the standard exploitation toolkit: modules, payloads and sessions, aimed at a service you already proved weak - SQLMap automation for confirmed SQLi: extract data once you have proven the injection by hand - hashcat for password attacks: recovering passwords from hashes - Engagement cleanup and hygiene: kill sessions, remove what you uploaded, restore configs, delete accounts you made, and leave a written cleanup log - LLM application security: prompt injection read against the OWASP Top 10 for LLM Applications, a lab chatbot fuzzed and tested for system-prompt leakage the same way you would test any API - Graded eJPT prep quiz 3 (Host and Network Penetration Testing)

Phase 4 · Blue Team, Reporting & Career (Weeks 10–12, 30 Hours)

WEEK	FOCUS AREA	TOPICS
Week 10	SIEM, SOC Workflow & GRC Basics	- A home SIEM built from a free stack, Wazuh, Splunk Free, or the Elastic Stack: an agent installed, a log source connected, and a first custom detection rule written and fired on purpose - The Windows Security log read for the event IDs a SOC actually watches (4624 logon, 4625 failed logon, 4672 special-privilege logon, 4688 process creation), local accounts, NTFS permissions, UAC, Firewall and Defender reviewed on a Windows 10/11 VM, then shipped into the SIEM and triaged as alerts - Active Directory structure (domain, OUs, domain controllers, GPOs) and its three credential-reuse attacks, pass-the-hash, Kerberoasting and AS-REP roasting, each recognised from the alert and log evidence it leaves rather than executed - A Tier-1 SOC shift worked for real: ticket-queue triage, escalation criteria, a clean handover note, and an AI-drafted triage

WEEK	FOCUS AREA	TOPICS
		summary checked line by line against the raw log before anyone trusts it - CWE, CVE and CVSS v3.1 scoring by hand, a finding entered on a risk register and checked against a policy or compliance document, with Nepal's NRB IT guidelines read where a BFI client would need them
Week 11	Capstone Assessment & Professional Reporting	- Capstone kickoff: scope review and evidence plan agreed before testing - Execute scoped VAPT on PortSwigger Labs / Juice Shop / trainer target - Report writing: executive summary, findings, CVSS, remediation - Peer review and trainer feedback, with every challenged finding defended out loud - The report assembled from the vault you have kept since Week 1: evidence pulled by link, not hunted for in a screenshots folder - Adjacent domains you must scope honestly instead of bluffing: mobile pen-test (static versus dynamic analysis, OWASP MASVS, when to hand off), cloud security on AWS (IAM misconfigs, exposed S3 and EC2, where cloud meets VAPT scope, full depth in TR-03) and incident response (clean evidence handoff so a defender can pick it up) - Attack-path reasoning: chain low-severity findings into one serious break-in, then build a phased 30/60/90-day remediation plan the client can execute
Week 12	Portfolio, Certifications & Career Launch	- Bug bounty workflow: HackerOne and Bugcrowd programmes, scope rules, severity tiers and payout tables - Responsible disclosure: coordinated timelines, no-programme cases, legal safe harbours - Writing good bounty reports: reproduction steps, impact, CVSS justification, proof-of-concept; what gets triaged vs rejected - Public writeups (responsibly redacted) - Resume, LinkedIn, GitHub for security roles - A timed live task first, AI tool open on the shared screen and choices narrated out loud, then mock security analyst + pen-tester interviews, plus a closing 1:1 with your mentor that works through the action list from the Week 6 midpoint review, item by item - Certification roadmap (Security+ → eJPT → CEH → OSCP; Security+ is currently SY0-701, due to retire around late 2026, so check CompTIA for the current version; this course runs no

WEEK	FOCUS AREA	TOPICS
		dedicated CEH exam-prep track, but its OWASP methodology and tool chain map onto CEH's syllabus, making it the natural next certification once eJPT is sat; OSCP now also issues as OSCP+, which expires after three years); book and sit eJPT (from INE Security) during the course (USD 200–250, 48-hour live lab exam, 35 practical questions, 70 percent pass; the 2026-refreshed eJPT added more web-app testing, recon and responsible AI use, all already drilled here), the best practical match for VAPT - Graded eJPT domain mock across all four exam domains (assessment methodologies, host and network auditing, host and network penetration testing, web-app penetration testing) - Career planning

Skills You Will Gain

CATEGORY	TECHNOLOGIES
Recon & Traffic	Nmap, Wireshark, httpx, subfinder, Google Dorks, Shodan, theHarvester
Web VAPT	Burp Suite, PortSwigger Labs, Juice Shop
Exploitation	Metasploit, SQLMap, hashcat, SMB/FTP/SSH service attacks
Hardening & Audit	Linux hardening, Windows hardening, auditd, file-integrity baselines (sha256sum, AIDE)
Windows & AD	Windows Security log (4624/4625/4672/4688), NTFS, UAC, Defender, Active Directory structure and attack paths
Blue Team & GRC	Wazuh, Splunk Free, Elastic Stack home SIEM, Tier-1 alert triage, CVSS v3.1 risk-register scoring
Scanners	nuclei, httpx (ProjectDiscovery), OpenVAS (Greenbone Community Edition), Nikto
Notes & Reporting	Obsidian or Notion engagement vault, HackTricks service playbooks
Scripting	Bash recon + log-triage scripts, Python (requests) for API probing
Labs	Kali Linux, VirtualBox, TryHackMe and HackTheBox free tiers

CATEGORY	TECHNOLOGIES
Frameworks	OWASP Top 10:2025, OWASP API Top 10 (2023), CVSS v3.1, MITRE ATT&CK
Bug Bounty	HackerOne, Bugcrowd platform rules, responsible disclosure
AI Assistants	ChatGPT for report drafting, recon synthesis, CVSS explanation and LLM application security testing

Topic Depth and Awareness

FOCUS AREA	LEARNING FOCUS
Networking, recon (Nmap, Wireshark, httpx)	Depth
OSINT (Google dorks, Shodan, theHarvester)	Depth
How a web application is built (stack anatomy)	Depth
Web VAPT (Burp, OWASP Top 10:2025)	Depth
XXE and insecure deserialization (recognise + report)	Awareness
API VAPT (JWT, REST, GraphQL awareness)	Depth
Exploitation toolchain (Metasploit, SQLMap, hashcat)	Depth
Network service attacks (SMB, FTP, SSH)	Depth
Templated scanning (nuclei, httpx)	Depth
CVSS scoring and report writing	Depth
Note discipline (Obsidian or Notion vault)	Depth, mandatory
Linux hardening and host review	Depth
Bash and Python security scripting (working scripts)	Depth
Bug bounty workflow and responsible disclosure	Depth

FOCUS AREA	LEARNING FOCUS
Social engineering awareness	Awareness
Windows security model, hardening and event logs	Depth
Active Directory structure and common misconfigs	Depth
Active Directory attack paths (pass-the-hash, Kerberoasting, AS-REP roasting)	Recognised from SIEM log evidence in Week 10, no live AD exploitation
SIEM (Wazuh, Splunk Free, Elastic Stack, Sentinel)	Awareness intro in Week 5; hands-on home lab and Tier-1 workflow in Week 10
GRC basics (CVSS v3.1, risk register, policy/compliance)	Depth (Week 10)
LLM application security (prompt injection)	Depth (Week 9)
Wireless and mobile pen-test	Awareness
Cloud security (AWS)	Awareness (covered in depth in TR-03)
Incident response and forensics	Awareness

Project Pool

Each student picks **one** capstone (final project) in Week 7. The list changes from batch to batch:

#	PROJECT	FOCUS
1	PortSwigger Labs / Juice Shop full VAPT report	Web + API VAPT, OWASP Top 10:2025
2	Network service enumeration + scoped service-misconfig report	Nmap, Metasploit, reporting
3	OSINT target profile + attack-surface report	Google dorks, Shodan, theHarvester, passive recon

#	PROJECT	FOCUS
4	Bug bounty dry-run on a public programme (read-only scope review)	HackerOne/Bugcrowd scope analysis, finding write-up practice
5	CTF-style portfolio with 5–8 solved rooms	HackTheBox and TryHackMe free tiers
6	Trainer-scoped assessment	Whatever the brief requires

Career Paths & Trajectory

ROLE	TIMELINE	FOCUS
Junior Web/API VAPT Analyst / Tier-1 SOC Analyst	0–2 yrs	Web + API VAPT support, alert triage, reporting
Penetration Tester / Security Analyst	2–4 yrs	Own engagements, network pen-testing, red-team sub-tasks
Senior Pen-Tester / AppSec Engineer	4–7 yrs	Architecture review, custom tooling
Security Lead / Consultant	7+ yrs	Engagement leadership, client advisory

FAQ

What does Cybersecurity & Ethical Hacking cost and how do I pay?

NPR 36,750. You can pay in cash at our Old Baneshwor campus, by bank transfer, or with Fonepay. Email info@saarathiacademy.com.np to ask about a payment plan.

Do I need prior experience?

No. The Gate Assessment before Day 1 shows where you are starting, and there is no pass or fail. If you are below the basics listed above, we suggest a short foundation course first.

How long is the course?

12 weeks (3 months). In Week 6 you get a private 1:1 review with your mentor and a written list of things to improve. In the final week you do a 1:1 mock interview and close that list.

What tools will I use?

You use **Kali Linux, Burp Suite, Metasploit, Wireshark, Nmap, SQLMap, nuclei and httpx**. You must also keep notes in an **Obsidian** or **Notion** vault from Day 1. Each phase ends with a piece for your portfolio: a recon report, a hardening audit, a web and API VAPT report, and the capstone report.

What roles does this prepare me for?

Junior Web/API VAPT Analyst and Tier-1 SOC Analyst. Network pen-testing jobs come later, after eJPT and more lab practice. We do not promise jobs. We build your portfolio, run mock interviews, improve your CV and LinkedIn, and refer you to companies in our hiring network.

How does the batch and mentorship work?

Each batch has at most 10 students, and each one gets direct mentor time and project reviews. Classes are in person at Old Baneshwor. Recordings and office hours are online. The Sunday Open Classroom is free for enrolled students.

Enrollment

- **Next Batch:** see the live course page
 - **Location:** Old Baneshwor Chowk, Kathmandu, Nepal
 - **Mode:** Online + Offline
 - **Contact:** 9744442469, 9761095364
 - Each batch has only 10 seats.
-

Cybersecurity & Ethical Hacking — full details, fees and next batch dates:
saarathiacademy.com.np/cybersecurity-course-in-nepal

Version 2.0 · Updated 11 Ashwin 2083