TR-11

Advanced Security

COURSE BRIEF

SKILLS & TOOLS YOU WILL MASTER

Kali + Burp Suite | Metasploit + BloodHound | AWS Security + IAM | Falco + Wazuh | MITRE ATT&CK

10 Reasons This Works.

Why students choose Saarathi - and how each card helps you ship a real career.

01

10 Max / Batch

Not 50. Not 30. Ten. Every student seen, heard, and unblocked - every class.

02

Sunday Open Classroom

Every Sunday the classroom is open. Come in, pair-program, get unstuck, or just focus.

03

Weekly Detailed Syllabus

Full syllabus from day one. Every week: what to read, what to build, what the outcome is.

04

Revision Every 5th Day

Every fifth class is a revision session. Nothing piles up or slips through.

05

Week 1: Mindset

The first week is about getting into the right headspace before touching a line of code.

06

3 Ways of Learning

Self-learning + collaboration + mentorship. All three built into every course.

07

1:1 Mock Interview

Real mock interview with your mentor in the final week. Actual hiring prep, not fluff.

08

CV + LinkedIn

Resume writing and LinkedIn optimisation. Leave with a profile that gets replies.

09

Real Projects

Every course ends with a deployed, publicly accessible project you can show employers.

10

Gate Assessment

Aptitude test before Day 1. Maps your strengths, weaknesses, learning style, and pace - then builds your personal plan.

saarathiacademy.com.np/advanced-security-course-in-nepal +977-9744442469 · +977-9761095364

Advanced Security

Why This Course

The security market has bifurcated. Junior pen-testers and SOC analysts are abundant; engineers who can run a red-team engagement, model cloud threat surfaces, build zero trust policy-as-code, and operate runtime detection-and-response pipelines are still rare and in demand both in Nepal and on remote international teams. Pay scales with your skills, portfolio, and whether you work locally or for international/remote clients. We don't promise a salary.

This is an advanced, coming-soon track. It assumes you already finished TR-04 or carry equivalent junior-VAPT experience, so it does not restart from beginner ground. Instead the first third of the course is a deliberate advanced on-ramp: it re-lays the primitives at engagement depth, settles the shared vocabulary, has you build your own attack lab, and teaches the assume-breach threat model that everything later depends on. Ground first, then intensity.

The 14-week track then covers the full advanced stack: offensive security and red-team tradecraft built on a VAPT foundation, cloud security posture management on AWS, zero trust architecture with OPA and policy-as-code, and runtime threat detection with Falco, Wazuh, and an ELK-backed SIEM. Every offensive technique is taught alongside the artefacts it leaves and the MITRE ATT&CK technique it maps to. You graduate ready for junior cloud security and detection engineering roles and as a credible OSCP or PNPT candidate, because the best defensive engineers are the ones who understand how attacks work from the inside. The full penetration-tester title is a 2 to 4 year trajectory this course sets you on, not a graduation badge.

Prerequisites are real. Students who come in without solid networking, Linux, and scripting experience will struggle even through the on-ramp. TR-04 (Ethical Hacking & VAPT) or an equivalent background is the intended starting point.

Who Is This Course For

- **TR-04 or equivalent graduates** who want to specialise beyond junior VAPT
- **Security analysts / SOC analysts** moving into offensive or engineering roles
- **DevOps engineers** adding a security posture management discipline
- **Cloud engineers** who need to own security architecture decisions, not just implement IAM policies
- **Developers** targeting product-security or platform-security engineering roles

Course Snapshot

PARAMETER	DETAILS
Course Code	TR-11
Duration	14 Weeks (3.5 Months)
Schedule	Monday to Friday, 2 Hours/Day
Total Hours	140 Hours
Batch Size	Maximum 10 Students
Course Fee	NPR 55,500
Level	Advanced (assumes TR-04-level junior pentest background)
Delivery	Online (live cohort)
Status	Coming Soon, waitlist open
Outcome	Junior Cloud Security / Detection Engineer; OSCP/PNPT candidate (pentester is a 2 to 4 year trajectory)

Prerequisites

- This one is not a beginner track. TR-04 (Ethical Hacking & VAPT) or equivalent hands-on VAPT experience with Burp Suite and Metasploit
- Solid TCP/IP and networking fundamentals, including the OSI model, DNS, HTTP and firewalls
- Linux command line at an operational level, file system, permissions, services and scripting
- Working Python or Bash scripting, you can read and modify an existing script
- A laptop with 8GB+ RAM and 50GB+ free disk space for the lab VMs
- Before Day 1: create a free-tier AWS account at aws.amazon.com/free. It needs a card to verify and can take a day to activate
- Saarathi Gate Assessment before Day 1, covering networking, Linux, scripting and VAPT fundamentals

Kali Linux and the rest of the lab environment are set up in the first class.

Assessments at a glance

Two exams bracket the course. The **Saarathi Gate Assessment** runs before Day 1 as a diagnostic with no pass or fail; it maps your learning style and pace. The **Saarathi Certification Exam** is sat at the end of the course, 2 hours and around 30 questions specific to this course in mixed formats (single choice, multi-select, true/false, numeric, ordering, matching, fill-in-the-blank, short or long answer, code where relevant, and short case studies). Pass mark is 60 percent and a pass is mandatory for the Saarathi Certificate of Completion. The exam is camera proctored: a working webcam must stay on for the full two hours, and stills are saved for your trainer to review. You can answer the questions in any order and come back to any of them, but every question needs an answer before you submit. Recommendation letters are discretionary, mentor-issued only to learners who pass the Certification Exam, and never guaranteed.

Your Learning Week

DAY	ACTIVITY
Mon–Fri	2-hour live session with labs
Mon–Fri	2-hour self-study (PentesterLab, TryHackMe, HackTheBox, CloudGoat; BTL1/SAL1 prep labs from Week 9)
Sunday	Open classroom for questions and focused lab work
Day 5 (every week)	Within the 2-hour session, the last 1 hour is a built-in revision block plus lab debrief for consolidation and doubt-clearing

> Security is learned by breaking things in a controlled environment. The live sessions introduce the technique; the daily lab hours build the instinct.

Week-by-Week Curriculum

Phase 1 · Offensive Foundations, Red Team Tradecraft & Cloud Grounding (Weeks 1–5, 50 Hours)

> **The advanced on-ramp (over a third of the course).** Phase 1 is the deliberate foundation for an advanced cohort: shared vocabulary, the assume-breach threat model, your own attack lab, the assumed TR-04 primitives revisited at engagement depth, and the AWS security model built before anything is broken. Sequenced gently on purpose, recon and enumeration before exploitation, but not beginner content.

WEEK	FOCUS AREA	TOPICS
Week 1	Advanced Offensive Methodology, Lab Build & OPSEC	- Why a red-team engagement differs from a noisy pen-test, and write the rules that bound it (red-team vs pen-test scoping distinctions) - Build your own attack lab from scratch (**Kali** attacker box, a Windows **Active Directory** domain, isolated network) - Learn the assume-breach threat model and the kill chain everything later builds on - Plan the attack around how a real adversary behaves (threat modelling with **MITRE ATT&CK v19**, the public catalogue of attacker tactics and techniques) - Keep your attacker setup unattributable (**OPSEC** for engagements, infrastructure separation, aged burner domains) - Passive target-picture building, certificate-transparency subdomains, org charts and metadata, written up as a profile (advanced **OSINT**: **LinkedIn** recon, DNS history, metadata extraction)
Week 2	Active Directory Enumeration & Kerberos Attacks	- Active Directory internals refreshed at attack depth (domains, trusts, **Kerberos** vs NTLM) - Map every route from low-privileged user to Domain Admin (AD enumeration with **BloodHound CE** v8 and its collector **SharpHound**, now also Entra ID / hybrid paths) - Pull crackable hashes from service accounts (**Kerberoasting** and **AS-REP roasting**) - Crack them on your own machine (offline cracking with **Hashcat**) - Escalate via misconfigured permissions and **Kerberos** delegation (ACL abuse; constrained, unconstrained, resource-based delegation)
Week 3	Exploitation, Post-Exploitation, Lateral Movement & C2	- Payloads that slip past antivirus and EDR (payload evasion: encoding, staged vs stageless, **Msfvenom**, in-memory shellcode runners) - Land on a host and harvest credentials (post-exploitation: **Mimikatz**, **LaZagne**, persistence, artefact tracking) - Move sideways with stolen credential material and pivot subnets (**pass-the-hash**, **pass-the-ticket**, credential replay, SSH tunnels, **proxychains**, SOCKS proxies)

WEEK	FOCUS AREA	TOPICS
		- Forge tickets and pull every domain hash (**Golden/Silver Ticket**, **DCSync**, full-domain persistence) - Stand up a command-and-control server and run quiet beacons (C2 framework setup with **Sliver**, **Havoc** or **Mythic**, beacon management)
Week 4	Web Application Red Teaming & Phase 1 Capstone	- Push injection past TR-04 basics into stored and blind variants (advanced injection chains: second-order **SQLi**, time-based, out-of-band) - Turn a server-side request forgery into stolen cloud credentials (**SSRF** to internal pivoting, cloud metadata endpoint abuse) - Breaking delegated sign-in flows (**OAuth**/**OIDC** attacks, token theft, consent phishing) - Combine small bugs into one critical attack path (chaining low-severity issues to high impact) - Phase 1 Capstone: red-team recon plus AD attack simulation report
Week 5	AWS Security Fundamentals & Posture Management	- Reason about who-can-do-what in AWS (**IAM** deep dive: roles, policies, permission boundaries, SCPs) - Cut access to the minimum needed (least-privilege design patterns, **IAM** policy simulation) - Control traffic in a private cloud network (**VPC** security: NACLs, Security Groups, flow logs) - Lock down cloud storage against leaks (**S3** security: bucket policies, ACLs, block-public-access, encryption) - Wire up the AWS services that flag suspicious activity (**CloudTrail**, **Config**, **GuardDuty**: the detection trio)

Phase 2 · Cloud Security & Zero Trust Architecture (Weeks 6–8, 30 Hours)

WEEK	FOCUS AREA	TOPICS
Week 6	Cloud Threat Modelling & Offensive AWS	- Trace how one small mistake snowballs into full account compromise (compounding cloud misconfigurations) - Steal a server's temporary cloud credentials, then apply the fix (**SSRF** to EC2 instance metadata, **IMDSv1** vs hardened **IMDSv2**) - Climb from weak identity to full admin, why identity is the #1 cloud attack surface in 2026 (**IAM** privilege escalation, `iam:PassRole` chains, **Pacu** and **CloudFox**,

WEEK	FOCUS AREA	TOPICS
		pathfinding.cloud references) - Find exposed cloud storage (**S3** data exposure patterns and detection) - Score an account against a hardening baseline and place it in the CSPM/CIEM/**CNAPP** market (**AWS Security Hub**, **CIS Benchmark** scoring, **Prowler** scans)
Week 7	Zero Trust Architecture & Policy-as-Code	- Design access trusting nothing by default (zero trust principles: verify explicitly, least privilege, assume breach) - Anchor security on identity, not network location (identity-centric security: **SAML**, **OIDC**, **mTLS**, certificate management) - Write access rules as code (**Open Policy Agent**/**OPA**, **Rego** language fundamentals) - Block unsafe **Kubernetes** deployments at the gate (write and test **OPA** policies for admission control) - Enforce a hardening baseline on every code change (**CIS Benchmarks** mapped to **OPA** policies in CI)
Week 8	Infrastructure-as-Code Security	- Catch cloud misconfigurations in infrastructure templates (**Terraform** and **CloudFormation** security scanning) - The main IaC scanners run and findings triaged (**Checkov**, **tfsec**, **KICS** for static analysis) - Stop passwords and keys entering the codebase (secrets in code: **trufflehog**, **git-secrets** detection) - Inventory software parts and track known vulnerabilities (**SBOM**/Software Bill of Materials with **Syft**, dependency CVE tracking with **Grype** or **Trivy**) - Map findings to Nepali bank audit rulebooks (Compliance & GRC: **ISO 27001**, **PCI-DSS**, NRB IT/cyber-resilience mapping) - Phase 2 Capstone: AWS threat model plus **OPA** policy suite for a realistic architecture

Phase 3 · Runtime Security, SIEM & SOAR (Weeks 9–12, 40 Hours)

WEEK	FOCUS AREA	TOPICS
Week 9	Container & Kubernetes Security	- Shrink what an attacker can do in a container (attack surface: image hardening, rootless containers) - Lock down cluster permissions and traffic (**Kubernetes RBAC**, pod security standards, network policies) - Detect attacks at runtime (**Falco** installation, default ruleset,

WEEK	FOCUS AREA	TOPICS
		custom rule authoring) - That detection run live (**Falco** in **Kubernetes**, capturing runtime alerts) - Block vulnerable images before they ship (**Trivy** image vulnerability scanning in CI)
Week 10	Host-Based Detection with Wazuh	- Roll host monitoring across a fleet (**Wazuh** agent deployment, manager configuration) - Turn noisy host events into real alerts (custom detection rules in **Wazuh**'s XML rule syntax) - Watch for changed files and rootkits (file integrity monitoring, rootkit detection, vulnerability assessment) - Feed alerts into a central log platform (**Wazuh** with a **SIEM** backend) - Treat detection rules like production code, reviewed and tested, in the portable **Sigma** format (detection-as-code workflow)
Week 11	SIEM Detection Engineering & SOAR	- Stand up log search and dashboards (**ELK** stack: **Elasticsearch**, **Logstash**, **Kibana**, or **OpenSearch**) - Pull logs from many sources into one shape (log ingestion pipelines: syslog, JSON, structured logs, Grok parsing onto Elastic Common Schema/**ECS**) - Write rules that spot multi-step attacks as portable **Sigma** rules (detection engineering: correlation, threshold, sequence rules) - Automate first response to alerts (**SOAR** playbooks with **Shuffle** or **n8n**: enrichment, containment, ticketing) - Attack your own stack to prove detections fire (purple teaming with **Atomic Red Team**: validate detection coverage)
Week 12	Incident Response & Threat Hunting	- An incident run end to end (IR phases, **PICERL**: preparation, identification, containment, eradication, recovery, lessons learned) - Hunt attackers who have not tripped an alert (threat hunting, hypothesis-driven queries in **ELK**) - Map detections against known adversary behaviours (**MITRE ATT&CK v19** navigator with the new Detection Strategies and Analytics, charting coverage of TTPs: tactics, techniques and procedures) - Capture memory and disk images, at awareness level (forensic triage: memory acquisition, disk imaging)

WEEK	FOCUS AREA	TOPICS
		- Sit a practice blue-team exam readiness check (**BTL1**/**SAL1** mock investigation) - Phase 3 Capstone: full detection stack demo with a simulated attack campaign

Phase 4 · Capstone & Career (Weeks 13–14, 20 Hours)

WEEK	FOCUS AREA	TOPICS
Week 13	Full Red-Team Engagement Simulation	- A full scoped engagement run end to end (recon, initial access, lateral movement, objective) - Stay quiet throughout (**OPSEC** discipline: no out-of-scope noise, clean artefact trail) - Write the client-grade debrief (format: narrative, TTPs mapped to **ATT&CK**, remediation) - Run live against classmates (purple-team session: blue team defends, red team attacks)
Week 14	Portfolio, GRC, Certifications & Career Launch	- Package proof of your skills for employers (security engineering portfolio: reports, tools, writeups) - Show your work satisfies Nepali bank audit rulebooks (Compliance & GRC: **ISO 27001** controls, **PCI-DSS**, NRB IT/cyber-resilience mapping) - Pass an entry certification and plan the bigger ones (**BTL1** or **SAL1** in-course; runway for **OSCP**/**PNPT**, **AWS SCS-C03**, **CKS**) - Present your red-team report and detection capstone (demo day, 1:1 mock interview) - Plan where to find work (career strategy: remote security roles, Nepal market, freelance consulting)

Skills You Will Gain

CATEGORY	TECHNOLOGIES
Offensive / Red Team	Kali Linux, Metasploit, Burp Suite, BloodHound CE, Sliver/Havoc/Mythic C2, Pacu
Cloud Security	AWS Security Hub, Prowler, Pacu, CloudFox, CloudTrail, GuardDuty, IAM

CATEGORY	TECHNOLOGIES
Zero Trust & Policy	Open Policy Agent (OPA), Rego, SAML, mTLS, CIS Benchmarks
Runtime Detection	Falco, Wazuh, Trivy
SIEM / Threat Hunting	ELK Stack / OpenSearch, Sigma, detection-as-code, MITRE ATT&CK v19 navigator
IaC Security	Checkov, tfsec, KICS, trufflehog
Active Directory & Entra ID	BloodHound CE, SharpHound, pass-the-hash, Kerberoasting, Golden Ticket

Topic Depth and Awareness

FOCUS AREA	LEARNING FOCUS
Advanced offensive exploitation and evasion	Depth
Active Directory attack chains (BloodHound, Kerberoasting)	Depth
AWS cloud security posture management	Depth
Zero trust architecture with OPA and Rego	Depth
Falco runtime security and custom rules	Depth
Wazuh detection engineering	Depth
SIEM detection rule writing (ELK / OpenSearch)	Depth
Purple teaming and ATT&CK mapping	Depth
IaC security scanning (Checkov, tfsec)	Depth
Container and Kubernetes security hardening	Depth
SOAR playbook automation	Awareness
Forensic triage and memory acquisition	Awareness
Commercial EDR bypass and licensed C2 (Cobalt Strike)	Awareness

Project Pool

Each student picks **one** capstone theme in Week 13. Pool rotates per batch:

#	PROJECT	FOCUS
1	Full red-team simulation report on a lab AD environment	Offensive, ATT&CK mapping, professional report
2	AWS cloud security posture audit with OPA policy suite	Prowler, Security Hub, Rego policies
3	Detection engineering portfolio: custom Falco + Wazuh rules + ELK dashboards	Runtime security, SIEM
4	Zero trust architecture design and policy-as-code implementation	OPA, CIS Benchmarks, CI enforcement
5	Trainer-scoped engagement	Whatever the brief requires

Career Paths & Trajectory

ROLE	TIMELINE	FOCUS
Junior Cloud Security / Detection Engineer	0–2 yrs	Cloud posture, runtime detection, VAPT support
Penetration Tester / Cloud Security Architect	2–4 yrs	Full engagements, architecture reviews
Senior Security Engineer / Red Team Lead	4–7 yrs	Platform security, custom tooling, engagement leadership
Security Principal / CISO Track	7+ yrs	Strategy, board reporting, programme ownership

FAQ

What does Advanced Security cost and how do I pay?

NPR 55,500 for 14 weeks. Classes run Monday to Friday, 2 hours a day, and on the fifth day the last hour is a built-in revision and doubt-clearing block, so it is 9 hours of new teaching and 1 hour of consolidation each week (140 contact hours total). Pay by cash, bank transfer, or

Fonepay. Email info@saarathiacademy.com.np for the payment plan.

Do I need prior experience?

Prerequisites are listed above. The Saarathi Gate Assessment runs before Day 1 to map your starting point, diagnostic, not pass-or-fail. Below prerequisites? We suggest a short foundation track first.

How long is the course?

14 Weeks (3.5 Months). A capstone project follows the guided phase, with a 1:1 mock interview in the final week.

What tools will I use?

Kali Linux, Metasploit, Burp Suite, BloodHound CE, Sliver/Havoc/Mythic C2, Pacu, Falco, Wazuh, OPA, AWS Security Hub, ELK/Sigma, all mapped to MITRE ATT&CK v19. Every module ships a public, deployed artefact for your portfolio, no toy projects.

What roles does this prepare me for?

Roles are listed in the Career Paths section. We do not promise jobs. We build your portfolio, run mock interviews, polish your CV and LinkedIn, and refer you into our hiring network.

How does the batch and mentorship work?

Maximum 10 students per batch, every student gets direct mentor time and project review. Delivered online as a live cohort, with session recordings and office hours. Sunday Open Classroom is free for enrolled students: pair-program, get unstuck, or just focus.

Enrollment

- **Status:** Coming Soon, join the waitlist at saarathiacademy.com.np/advanced-security-course-in-nepal
- **Mode:** Online (live cohort)
- **Contact:** 9744442469, 9761095364
- Limited to 10 seats per batch

Advanced Security — full details, fees and next batch dates: saarathiacademy.com.np/advanced-security-course-in-nepal

Version 1.0 · Updated July 2, 2026