Ethical Hacking & Network Security

Learn Security Methodically, Test Responsibly, Report Professionally

This course is designed for disciplined entry-level learners who want to understand how attackers find weaknesses and how defenders respond without hype, shortcuts, or unsafe classroom behaviour. In 12 weeks, you build foundations in networking, Linux hardening, web and API testing, controlled vulnerability assessment, and professional reporting.

All offensive work stays inside approved practice environments from Day 1. The aim is not performative hacking. The aim is learning how to investigate safely, verify carefully, and communicate risk clearly.

Why This Course?

The Market Reality

Global Context: Organizations continue to face phishing, credential abuse, exposed services, weak web applications, and fragile configurations. They need security professionals who can test responsibly, verify carefully, and communicate findings clearly.

Nepal Context: Banks, fintech products, websites, hosting environments, and growing digital businesses in Nepal all need stronger security review habits. The gap is not only in tooling; it is in methodology, validation, and reporting discipline.

Your Opportunity: This course positions you for **security analyst, junior penetration testing, vulnerability review, and application-security support roles**. You graduate with portfolio evidence that shows method, classroom discipline, and reporting ability - not just screenshots of tools.

Nepal-Relevant Reality	Opportunity
Web defacement, weak passwords, and exposed services still happen regularly	Security review skills stay practical and relevant
Many learners know tools by name but cannot explain methodology	You gain a more credible, job-ready foundation
Local companies need safer app and infrastructure review habits	Entry-level assessment and remediation support work can grow
Responsible security communication is still rare	Clear reporting becomes a real advantage

Course Snapshot

Parameter	Details
Course Code	TR-04
Title	Ethical Hacking & Network Security (Cybersecurity)
Duration	3 Months (12 Weeks)
Schedule	Monday to Friday (Mon–Fri, 5 Days/Week), 2 Hours/Day
Total Hours	120 Hours of Live Training
Batch Size	Maximum 10 Students
Course Fee	NPR 35,000
Prerequisites	Baseline digital literacy is required. You should already understand what a web browser, IP address, and file system are, be comfortable using a computer daily, and have a laptop with 8GB+ RAM and at least 50GB free disk space for labs and virtual machines. Before Day 1, complete TryHackMe's free Pre-Security learning path and our pre-course 7-day challenge. Saarathi Gate Assessment (diagnostic, no pass/fail) before Day 1.
Self-Study	Minimum 2 hours/day outside class (mandatory)
Outcome	Security Analyst / Junior Penetration Tester

Your Learning Week

Day	Activity
Mon–Fri	2-hour live class session (hands-on, classroom-based)
Mon–Fri	Minimum 2 hours self-study & classroom practice (mandatory)
Saturday	No classes - flexible self-study, peer collaboration, classroom work
Sunday	Whole day self-learn time. Classrooms remain fully open for you to come in, study, collaborate with peers, and build projects.

> *Every student must spend at least 2 dedicated hours a day on focused classroom practice beyond the classroom. Security skill comes from repetition, documentation, and careful review.*

Week-by-Week Curriculum

Phase 1: Security Mindset, Networking & Safe Practice (Weeks 1–3, 3 Weeks, 30 Hours)

Week	Focus Area	What You'll Master
Week 1	Security Mindset, Authorization & Lab Discipline	Scope, authorization, TCP/IP basics, packet capture basics, and disciplined evidence notes
Week 2	Network Services, Filtering & Traffic Analysis	DNS, HTTP/HTTPS, TLS, segmentation, firewalls, packet reading, and suspicious-pattern review
Week 3	Nmap, Enumeration & Secure Architecture	Scoped scanning, service review, attack-surface mapping, and safer architecture basics

Phase 2: Linux Hardening & Host Review (Weeks 4–6, 3 Weeks, 30 Hours)

Week	Focus Area	What You'll Master
Week 4	Linux Hardening Fundamentals	Permissions, users, services, SSH hardening, firewall basics, and safer system setup
Week 5	Logging, Auditing & Integrity Checks	journald, auth logs, auditd, integrity review, suspicious indicators, and remediation note-taking
Week 6	Host Enumeration, Hardening Review & Mini Report	Service exposure review, tool-assisted validation, AppArmor and SELinux awareness, and documented host assessment

Phase 3: Web & API Security Testing (Weeks 7–9, 3 Weeks, 30 Hours)

Week	Focus Area	What You'll Master
Week 7	HTTP, Burp & Injection Fundamentals	HTTP/HTTPS, Burp workflow, OWASP thinking, SQLi, XSS, and safer testing habits
Week 8	Auth, Access Control & Misconfiguration	Authentication review, privilege boundaries, CSRF, session handling, and security misconfiguration
Week 9	API, Modern Web Testing & Proof Capture	REST/JWT testing, API enumeration, GraphQL awareness, SSRF awareness, and evidence capture for reporting

Phase 4: Validation, Reporting & Career Prep (Weeks 10–12, 3 Weeks, 30 Hours)

Week	Focus Area	What You'll Master
Week 10	Scanning, Enumeration & Triage	CVE/CWE/CVSS basics, support tools, false positives, validation habits, and attack-path reasoning
Week 11	Capstone Assessment & Professional Reporting	Controlled assessment workflow, executive summary writing, finding documentation, remediation roadmap, and presentation
Week 12	Portfolio, Interviews & Career Launch	Security resume, LinkedIn/GitHub polish, mock interviews, portfolio packaging, and next-step planning

Skills You'll Gain

Security Tools & Techniques

Tool/Technique	Proficiency Level
Wireshark	Packet analysis foundation
Nmap	Scoped enumeration and review
Burp Suite	Web and API testing workflow
OWASP Top 10	Vulnerability assessment foundation
Linux Hardening	Host review and defense habits
CVSS & Reporting	Risk prioritization and communication

Security Concepts

Concept	Application
Scope & Authorization	Ethical boundary for all security work
Attack Methodology	Structured recon, validation, and reporting
Evidence Quality	Requests, logs, packets, and proof capture
Remediation Planning	Fix recommendations and retest thinking

Topic Depth and Awareness

Section	Guidance
Purpose	This course separates what you must practice deeply from what you only need to understand with working awareness.
Depth	Scope discipline, packet analysis, Linux review, web/API testing, scanner triage, evidence capture, and report writing
Awareness	Wireless specialization, deeper container security, bug bounty strategy, and broader defensive frameworks
How to use this syllabus	Spend most of your self-study time on methodology, evidence quality, and repeated classroom execution before chasing extra tools.

Project Pool

> *All options below are **intermediate-level final projects**. Each student chooses **one** final project from this pool. Trainers may run smaller guided exercises during the course, but public phase-wise project sections are intentionally removed so the completion standard stays clear and consistent.*

#	Final Project Choice	What You Will Build	Core Stack / Tools
1	Network Mapping & Defense Review	Map exposed services, explain likely risk, and propose safer configurations with clear documentation.	Wireshark, Nmap, network mapping, documentation
2	Hardened Linux Platform	Secure a Linux system, review exposures, and document the changes clearly for later handoff.	Linux hardening, audit basics, access control, log review
3	Web Application Security Assessment	Run scoped OWASP-style testing and produce a professional report with prioritized findings.	Burp Suite, OWASP testing, manual testing, report writing
4	Internal Security Validation Assessment	Perform a structured internal assessment across recon, validation, and remediation notes without hype or guesswork.	Nmap, OpenVAS awareness, enumeration, risk reporting

#	Final Project Choice	What You Will Build	Core Stack / Tools
5	SecureBank Security Assessment	Conduct an authorized application and system assessment with evidence collection, risk scoring, and remediation handoff.	Scoped testing, CVSS, professional reporting, presentation

Career Paths & Trajectory

Role Path	Focus and Proof	Stage and Timeline	What Actually Matters
Security Analyst	Review network, host, and web findings with clear triage and remediation communication. Proof you leave with: Validation habits, reporting discipline, and calmer risk explanation	Entry role - first 0–12 months	Evidence quality, responsible scope handling, and knowing when a finding is real versus noisy.
Junior Penetration Tester / Vulnerability Analyst	Run scoped assessments and verify common web, API, and host weaknesses responsibly. Proof you leave with: Assessment write-ups, Burp and Nmap workflow proof, and CVSS prioritization habits	Growth role - 1–3 years	Strong methodology, safer testing habits, and reproducible reporting teams can act on.
Application Security Analyst / Security Engineer	Work with developers on secure fixes, repeat testing, and better prevention before release. Proof you leave with: Developer-facing remediation notes, web/API review confidence, and retest discipline	Specialist path - 3–5 years	Practical risk judgment, useful collaboration with engineering teams, and prevention instead of only detection.
Senior Security Engineer / Red-Blue Hybrid Specialist	Lead deeper assessments or defensive review programs without hype or scope creep. Proof you leave with: Portfolio assessments, attack-path reasoning, and stronger communication habits	Senior path - 5+ years	Trust, ethics, structured methodology, and the ability to explain security trade-offs to both engineers and leaders.

Saarathi Gate & Completion Review

Before You Start: Saarathi Gate Assessment

All students complete the **Saarathi Gate Assessment** before Day 1. It is a short diagnostic review of aptitude, learning behaviour, and thinking style. It has **no pass/fail** and is used only to tailor support from the start.

After Course Completion: Saarathi Completion Review

The **Saarathi Academy Certificate** is issued after the selected final project is completed, documented, and reviewed by the trainer. There is **no separate certification exam** for this course.

Completion Requirements:

1. **Attendance:** Minimum 80% attendance
2. **Weekly Work:** Core deliverables, revision work, and practice tasks completed
3. **Final Project:** One intermediate-level project selected from the project pool and completed to trainer-approved quality
4. **Portfolio Proof:** Screenshots, documentation, case-study notes, or equivalent proof assets updated
5. **Trainer Review:** Practical execution, consistency, communication, and overall growth signed off by the trainer

Enrollment & Next Steps

Next Batch: Starting soon (contact for exact dates) **Offline Location:** Old Baneshwor Chowk, Kathmandu, Nepal **Mode:** Online + Offline **Contact (Call/WhatsApp):** 9761095364, 9744442469

» **[ENROLL NOW]** - Limited to 10 seats per batch

Test safely, document evidence, and explain risk without hype.

Last Updated: Mar 30, 2026