RED TEAM · BLUE TEAM · MASTERY PATH

LVL 6
EXPERT DEFENDER

Becoming a Cybersecurity Expert

A complete roadmap from working software developer to professional-grade defender — able to break into hardened systems, hunt the attackers inside them, and close the holes for good.

▲ RED TEAM

Think like the adversary. Exploit, pivot, escalate, and prove the impact of every hole.

■ BLUE TEAM

Detect, respond, harden, and hunt. Defend the system before, during, and after an attack.

Md. Rajib Hawlader
Author & Curator

https://rajib.uk

ORIENTATION

The Mission & How to Reach Expert Level

> This is not a beginner skim. The goal is genuine **expert-level capability**: the ability to assess a protected system, find the holes a real attacker would use, exploit them in an authorized engagement, and then switch hats to detect, contain, and permanently defend against those same attacks. That dual capability — offense and defense — is what separates a hobbyist from a professional security engineer.

Why a Developer Has a Head Start

Most people entering security fight the fundamentals: code, networking, the command line, how applications actually work. You already own those. That foundation lets you skip past surface-level material and go straight to **how systems fail and how to defend them**. Your code-reading ability alone makes you a stronger vulnerability researcher and secure-code reviewer than most newcomers will ever be.

The Expertise Ladder

Expertise is built in deliberate layers. Each phase below assumes the previous one is solid. You don't reach "defend against any intrusion" by memorizing tools — you reach it by understanding attacker tradecraft deeply enough to predict, detect, and disrupt it.

Level	What you can do	Mindset
1 · Foundation	Understand attack surface, networking, the security model of apps	"How is this built?"
2 · Offensive Web	Find & exploit the OWASP-class vulns in web apps and APIs	"How do I break in?"
3 · Full Attack Chain	Recon → exploit → privilege escalation → pivot → persistence	"How far can I get?"
4 · Defense & Detection	Logging, SIEM, detection engineering, incident response	"How do I catch this?"
5 · Threat Hunting	Proactively hunt adversaries, map to MITRE ATT&CK, harden	"Who is already inside?"
6 · Purple Mastery	Run an emulated attack end-to-end and the detection that beats it	"I own both sides."

How to Use This Roadmap

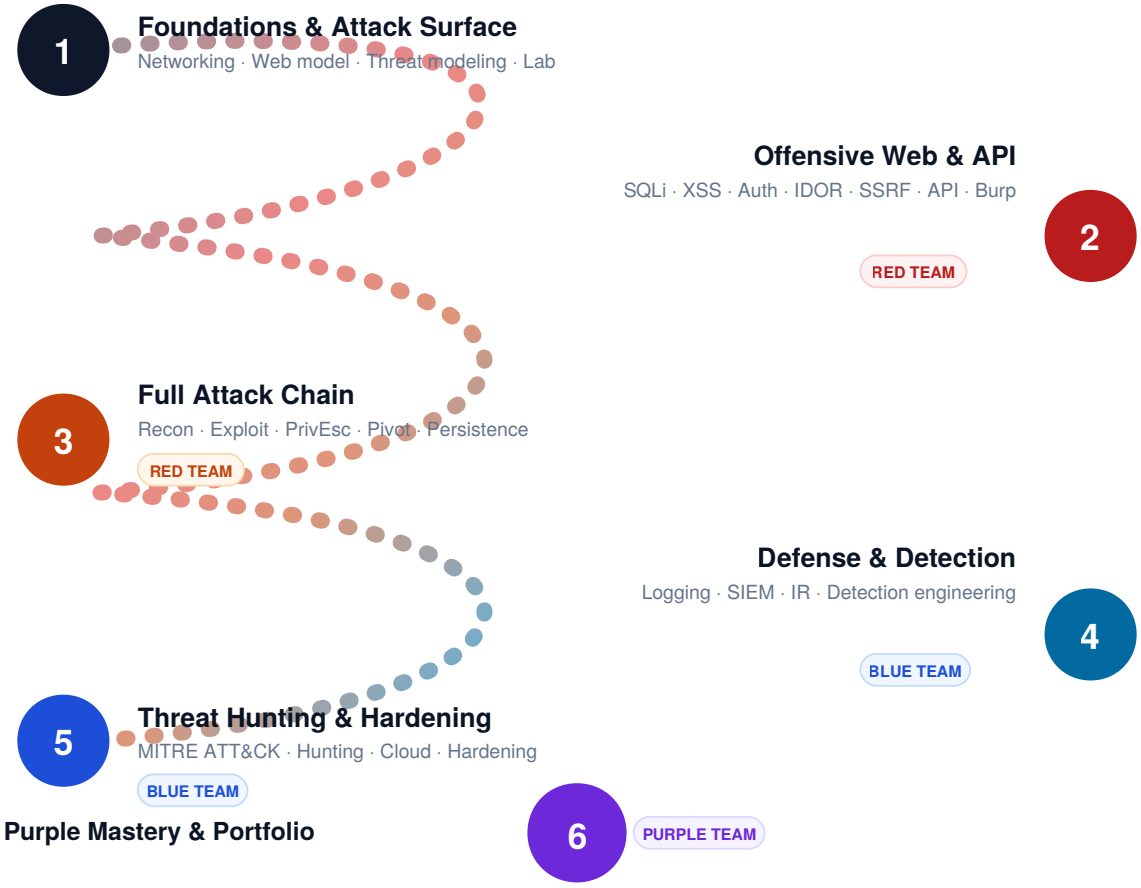
The plan runs in **6 phases over roughly 6 months** (extend or compress to fit your time — the original 3-month version maps onto Phases 1–3). Budget **12–18 hours per week**. Every phase has: what to learn, hands-on labs on free platforms, a red-team / blue-team split so you build both perspectives, AI tutor prompts, and a capstone milestone that proves the skill. **Everything required is free.**

Set up your AI tutor first. Give it a standing role so it teaches at expert depth instead of dumbing things down.

> "You are my cybersecurity mentor. I'm an experienced software developer training to red-team and blue-team level. For any topic: explain the attacker technique with a concrete example, map it to MITRE ATT&CK, then explain exactly how a defender detects and prevents it. Quiz me and challenge sloppy reasoning. Never give CTF/lab answers outright — guide me."

THE JOURNEY

Your 6-Phase Mastery Roadmap



01 **Foundations & Attack Surface** — **Weeks 1–3**
The security mindset, networking, web internals, threat modeling, lab build

02 **Offensive Web & API Exploitation** — **Weeks 4–8**
SQLi, XSS, auth/access control, SSRF/XXE, API & race conditions, Burp mastery

03 **Full Attack Chain (Red Team Core)** — **Weeks 9–13**
Recon, exploitation, privilege escalation, lateral movement, persistence, C2

04 **Defense, Logging & Detection (Blue Team Core)** — **Weeks 14–18**
SIEM, log analysis, detection engineering, incident response lifecycle

05 **Threat Hunting, Cloud & Hardening** — **Weeks 19–22**
MITRE ATT&CK, proactive hunting, cloud security, system hardening

06 **Purple Team Mastery & Portfolio** — **Weeks 23–26**
End-to-end attack + detection, secure code review, reporting, career launch

PHASE 01 · WEEKS 1–3

Foundations & Attack Surface

> Goal: build the mental model an expert uses to look at *any* system and instantly see how it could be attacked and defended. No tool-collecting yet — this is about how systems really work and where they break.

01 Foundations & Attack Surface

MINDSET · NETWORKING · WEB INTERNALS

LEVEL 1

CORE CONCEPTS TO MASTER

- **Security triad & beyond:** CIA, plus authentication, authorization, non-repudiation, defense-in-depth.
- **Networking for attackers:** TCP/IP, DNS, HTTP/HTTPS, TLS handshake, cookies, sessions, headers, NAT, firewalls.
- **The web security model:** same-origin policy, CORS, CSP — and how each becomes an attack vector when misconfigured.
- **Threat modeling:** assets, trust boundaries, attack surface, STRIDE. Model a system you've built.
- **OWASP Top 10 (2021)** as your vulnerability map; read it end to end.

HANDS-ON LABS

- Build your lab: VirtualBox + **Kali Linux** + an isolated host-only network. Snapshot it.
- Capture your own browser traffic in **Wireshark**; identify the TLS handshake and dissect an HTTP request.
- Complete TryHackMe's free **Pre Security** and **Network Fundamentals** paths.

TCP/IP | DNS | TLS | HTTP | STRIDE | OWASP Top 10 | Wireshark

AI Lab:

> `"Here is a raw HTTP request I captured. Walk through every header, tell me which an attacker could abuse and how, and what a defender would log to detect abuse."`

✓ **Milestone:** Produce a one-page threat model of an app you built, listing assets, trust boundaries, and the top 5 realistic attacks.

FREE RESOURCES

- **TryHackMe** — Pre Security path: tryhackme.com/path/outline/presecurity · Network Fundamentals: tryhackme.com/module/network-fundamentals
- **OWASP Top 10** — owasp.org/www-project-top-ten · Cheat Sheet Series: cheatsheetseries.owasp.org
- **Professor Messer** — free Network+ & Security+ courses: professormesser.com

- **Wireshark** — official docs: wireshark.org/docs
- **Kali Linux** — download & docs: kali.org/get-kali

PHASE 02 · WEEKS 4–8

Offensive Web & API Exploitation

> Goal: become genuinely dangerous against web applications and APIs — the largest attack surface in the modern world. By the end you can find and exploit every OWASP-class vulnerability by hand.

02 Offensive Web & API

INJECTION · AUTH · ACCESS · SSRF · API

RED · LEVEL 2

Week	Focus	Primary labs (free)
4	SQL injection — in-band, blind, time-based; defenses (parameterization)	PortSwigger SQLi path
5	XSS — reflected, stored, DOM; CSP; cookie/token theft	PortSwigger XSS path
6	Authentication & access control — IDOR, privilege escalation, JWT attacks	PortSwigger Auth + Access
7	SSRF, XXE, command injection, path traversal, insecure deserialization	PortSwigger SSRF/XXE/CMDi
8	API testing (BOLA, mass assignment), race conditions, business logic	PortSwigger API + Race conditions

▲ RED TEAM SKILL

- Drive everything through **Burp Suite** (Proxy, Repeater, Intruder) by hand before automating.
- Chain bugs: e.g. SSRF → cloud metadata → credential theft.
- Write a clean exploit PoC for each finding.

■ BLUE TEAM MIRROR

- For every vuln, write the **secure code fix** (you're the dev — this is your edge).
- Note what log entry / WAF rule would catch the attack.
- Add input validation & output encoding patterns to a reference doc.

AI Lab:

> `"Here's the payload that solved this blind SQLi lab. Explain why time-based was required vs UNION, rewrite the vulnerable query safely, and tell me the exact SIEM detection rule for this attack."`

✓ **Milestone:** Complete the full PortSwigger paths above and write one professional vulnerability report (title, CVSS, repro, impact, fix) for a chained exploit.

FREE RESOURCES

- **PortSwigger Web Security Academy** — the gold standard, fully free: portswigger.net/web-security
- **OWASP API Security Top 10** — owasp.org/API-Security
- **Burp Suite Community** — portswigger.net/burp/communitydownload · docs: portswigger.net/burp/documentation
- **PwnFunction** (XSS explained) — youtube.com/c/PwnFunction · **John Hammond** — youtube.com/c/JohnHammond010
- **PortSwigger YouTube** — youtube.com/c/PortSwiggerTV

PHASE 03 · WEEKS 9–13

Full Attack Chain — Red Team Core

Goal: move from single bugs to full intrusions. Learn the complete penetration testing lifecycle the way a real attacker (or red teamer) executes it — getting initial access, escalating, moving laterally, and persisting.

03 Full Attack Chain

RECON → EXPLOIT → PRIVESC → PIVOT → PERSIST

RED · LEVEL 3

THE KILL CHAIN YOU WILL MASTER

1. **Reconnaissance** — passive OSINT + active scanning. Master **Nmap** (host discovery, version detection, NSE scripts).
2. **Enumeration** — services, shares, web dirs (gobuster/ffuf), users.
3. **Exploitation** — exploit known services; intro to **Metasploit** framework (modules, payloads, handlers).
4. **Privilege escalation** — Linux (SUID, sudo, cron, capabilities; LinPEAS) & Windows (tokens, services, unquoted paths; WinPEAS).
5. **Lateral movement & pivoting** — credential reuse, tunneling, Active Directory basics (Kerberos, BloodHound concepts).
6. **Persistence & C2** — understand how attackers stay in; intro to command-and-control concepts (defensive awareness).

HANDS-ON LABS

- **Hack The Box "Starting Point"** + Academy free modules.
- **TryHackMe "Jr Penetration Tester"** / Offensive Pentesting rooms (many free).
- **Metasploitable 2/3** and vulnerable VMs *in your isolated lab only*.
- Active Directory attack labs (TryHackMe AD rooms) — most enterprise breaches go through AD.

Nmap | Metasploit | LinPEAS/WinPEAS | ffuf/gobuster | Active Directory | Pivoting

AI Lab:

> "Here's my LinPEAS output from a lab box. Don't tell me the answer — ask me guiding questions that lead me to the privilege-escalation path, and explain the ATT&CK technique it maps to."

✓ **Milestone:** Compromise an HTB/THM box from recon to root and write a full red-team report with the complete kill chain and remediation per step.

FREE RESOURCES

- **Hack The Box** — Starting Point: app.hackthebox.com/starting-point · Academy: academy.hackthebox.com
- **TryHackMe** — Jr Penetration Tester path: tryhackme.com/path/outline/jrpenetrationtester
- **GTFOBins** — gtfobins.github.io · **LOLBAS** — lolbas-project.github.io
- **Nmap book** (free online) — nmap.org/book
- **IppSec** (HTB walkthroughs) — youtube.com/c/ippsec

PHASE 04 · WEEKS 14–18

Defense & Detection — Blue Team Core

> Goal: now flip the board. You know how attacks work — learn to **see them happen and stop them**. This is where you become a defender who can protect a system against the very techniques you just learned.

04 Defense & Detection

LOGGING · SIEM · IR · DETECTION ENGINEERING

BLUE · LEVEL 4

CORE CAPABILITIES

- **Logging & telemetry:** what to log, where (endpoint, network, app), and Sysmon on Windows / auditd on Linux.
- **SIEM fundamentals:** ingest, parse, query, and alert. Learn **Splunk** (free training) and the **ELK** stack.
- **Detection engineering:** write detections as code with **Sigma** rules; understand true/false positives and detection tuning.
- **Network defense:** IDS/IPS concepts, **Snort/Suricata**, analyzing PCAPs in Wireshark for malicious traffic.
- **Incident response lifecycle:** Prepare → Identify → Contain → Eradicate → Recover → Lessons learned.

▲ USE YOUR RED KNOWLEDGE

- Replay attacks you learned in Phase 3 against your lab.
- Generate the malicious telemetry yourself, then go find it.

■ BUILD THE DETECTION

- Write a Sigma rule that catches each attack.
- Triage a simulated alert end-to-end and document the IR steps.

HANDS-ON LABS

- **Blue Team Labs Online** & **CyberDefenders** — free defensive challenges (log analysis, PCAP, malware triage).
- **TryHackMe SOC Level 1** path — Splunk, ELK, Sysmon, phishing analysis (free rooms available).
- Stand up a mini home SIEM: ship Sysmon logs into Splunk Free / ELK and alert on suspicious activity.

Splunk · ELK · Sigma · Sysmon · Suricata · Incident Response

AI Lab:

> `"I ran a Mimikatz-style credential dump in my lab. Here are the Windows event logs. Help me write a Sigma detection rule, explain which ATT&CK technique it covers, and how an attacker might evade it."`

✓ **Milestone:** Detect an attack you launched yourself — capture the telemetry, write a working detection rule, and produce an incident report with timeline and containment steps.

FREE RESOURCES

- **TryHackMe SOC Level 1** — tryhackme.com/path/outline/soclevel1
- **Blue Team Labs Online** — blueteamlabs.online · **CyberDefenders** — cyberdefenders.org
- **Splunk Free** — splunk.com/download · free training: splunk.com/training/free-courses

- **Sigma rules & docs** — github.com/SigmaHQ/sigma
- **Malware Traffic Analysis** (free PCAP exercises) — malware-traffic-analysis.net

PHASE 05 · WEEKS 19–22

Threat Hunting, Cloud & Hardening

> Goal: rise above reactive defense. Proactively hunt adversaries who evade alerts, map everything to a shared attacker framework, and harden systems so the holes don't exist in the first place — including in the cloud.

05 Threat Hunting & Hardening

ATT&CK · HUNTING · CLOUD · HARDENING

BLUE · LEVEL 5

CORE CAPABILITIES

- **MITRE ATT&CK** as your shared language: tactics, techniques, and mapping both attacks and detections to it.
- **Threat hunting:** hypothesis-driven hunts ("assume breach"), behavioral analytics, hunting with the Pyramid of Pain in mind.
- **Threat intelligence & IOCs:** consuming intel, recognizing TTPs, attribution basics.
- **Cloud security:** shared responsibility model, IAM misconfig, public buckets, exposed metadata (IMDSv2), and how web vulns chain into full cloud compromise.
- **System & network hardening:** CIS Benchmarks, least privilege, segmentation, patch & secrets management.

HANDS-ON LABS

- **flaws.cloud** & **flaws2.cloud** — free hands-on AWS attack/defense challenges.
- **Atomic Red Team** — execute ATT&CK techniques safely in your lab, then hunt them.
- Harden a lab VM against the CIS Benchmark and re-run your Phase 3 attacks to confirm they fail.
- Run a structured threat hunt on your SIEM data and document the hypothesis → query → finding.

MITRE ATT&CK | Atomic Red Team | Threat Intel | CIS Benchmarks | Cloud IAM | Hardening

AI Lab:

```
"Walk me through the Capital One 2019 breach as a chain of specific ATT&CK techniques.
For each step, give the exact control (IMDSv2, egress filtering, IAM least privilege)
that would have broken the chain, and a hunt query to detect it."
```

✓ **Milestone:** Run an Atomic Red Team technique, hunt it down in your own telemetry, then harden the system so the same technique is detected or blocked on the next run.

FREE RESOURCES

- **MITRE ATT&CK** — attack.mitre.org · ATT&CK Navigator: mitre-attack.github.io/attack-navigator

- **flaws.cloud** — flaws.cloud · **flaws2.cloud** — flaws2.cloud
- **Atomic Red Team** — github.com/redcanaryco/atomic-red-team
- **CIS Benchmarks** (free downloads) — cisecurity.org/cis-benchmarks
- **TryHackMe** — Cyber Defense path: tryhackme.com/path/outline/blueprimer

PHASE 06 · WEEKS 23–26

Purple Team Mastery & Portfolio

> Goal: prove you own both sides. A purple-team exercise — running a full attack *and* the detection that beats it — is the clearest demonstration of expert capability. This phase turns your skills into a portfolio that gets you hired.

06 Purple Team Mastery & Portfolio

FULL ATTACK + DETECTION · SECURE REVIEW · CAREER

PURPLE · LEVEL 6

CAPABILITIES TO CONSOLIDATE

- **Purple-team exercise:** emulate a realistic adversary end to end, then write and validate the detections that catch each step.
- **Secure code review at depth:** SAST/DAST in CI/CD; trace taint from source to sink. Run **Semgrep**, **Bandit**, **gitleaks**, dependency scanning.
- **CTF & sharpening:** PicoCTF, OverTheWire, live events on CTFtime to keep reflexes fast.
- **Professional reporting & ethics:** CVSS scoring, executive vs technical reporting, responsible disclosure, rules of engagement, and the law.

FINAL CAPSTONE (DO ALL FOUR)

1. Run a documented **attack-and-defend exercise** in your lab: compromise a target, then show the detection + hardening that defeats the same attack.
2. Publish a **GitHub portfolio**: lab write-ups, detection rules, a secure-code-review case study, CTF solutions.
3. Write one polished, professional **pentest report** and one **incident-response report**.
4. Start a security blog on your own site documenting the journey — exactly what hiring managers look for.

AI Review:

```
"Review my purple-team write-up and GitHub portfolio. As a hiring manager for a senior security engineer role, what's strong, what's weak, and what one project would make me competitive for both red-team and blue-team positions?"
```

✔ **Milestone:** A complete, public portfolio that demonstrates you can break into a hardened system *and* defend one — the definition of expert capability.

FREE RESOURCES

- **PicoCTF** — picoctf.org · **OverTheWire** — overthewire.org/wargames · **CTFtime** — ctftime.org
- **Semgrep** — semgrep.dev · **Bandit** — github.com/PyCQA/bandit · **gitleaks** — github.com/gitleaks/gitleaks
- **OWASP Dependency-Check** — owasp.org/www-project-dependency-check

- **MITRE Caldera** (adversary emulation) — github.com/mitre/caldera
- **FIRST CVSS calculator & guide** — first.org/cvss

Beyond 26 Weeks — Sustaining Expertise

Expertise is maintained, not finished. Pick a depth specialization (AppSec, red team, detection engineering, cloud security, or DevSecOps), keep one lab or hunt per week, follow active researchers, and work toward a respected certification when ready — the affordable **eJPT** for hands-on pentesting, the free **Security+** objectives for breadth, or **BTL1**-style defensive paths. Your developer foundation plus this dual red/blue capability already puts you ahead of most professionals; consistency and depth carry you the rest of the way.

Ethical Use — Read This

Every technique in this guide is provided strictly for **education and authorized, legal security testing**. Only test systems you own or have explicit written permission to assess, and always operate within an agreed scope and rules of engagement. Unauthorized access to computer systems is a serious criminal offense in virtually every jurisdiction. Build and attack only in isolated, deliberately vulnerable lab environments. The capability to break into systems carries the responsibility to use it lawfully and to make systems safer — that is the entire point of becoming an expert defender.

Copyright & Disclaimer

Author: **Md. Rajib Hawlader** | Website: **https://rajib.uk**