

M I L E S T O N E C A R E E R R O A D M A P

VAPT

Vulnerability Assessment & Penetration Testing

A complete, step-by-step, operational guide for college students and fresh graduates

7 Milestones · 30+ Action Steps · 20 References

For College students & fresh graduates	Duration 3-5 years to senior level	Focus Offensive security & VAPT	Frameworks OWASP · PTES · MITRE ATT&CK
---	---------------------------------------	------------------------------------	---

How to Use This Roadmap

This roadmap is structured as 7 sequential milestones. Each milestone has a concrete entry condition, a set of numbered action steps, and a clear exit deliverable - the proof that you have completed it and are ready to move forward.



Critical principle

Never skip a milestone. Every step builds directly on the last. Jumping to advanced penetration testing without foundational networking knowledge is the single most common reason people give up. The roadmap is sequential by design.



The golden rule of VAPT careers

Employers hire demonstrated ability, not course completion certificates. Every milestone must produce a visible, verifiable artifact - a report, a GitHub profile, a rank on a platform, a finding. If you can't show it, it doesn't count.

Full Journey Overview

Milestone	Name	When	Key Deliverable
M1	Foundation: How Everything Works	College Year 1-2	Home lab running + THM Pre-Security complete
M2	Core Skills: Offense & Defense	College Year 2-3	HTB 'Hacker' rank + first CTF solve
M3	Application Security Deep Dive	College Year 3 / Final year	OWASP Top 10 lab - all 10 exploited
M4	Portfolio & First Real Experience	Final year + graduation	Public writeups + sample pentest report
M5	Land Your First Role	0-6 months post-grad	Signed offer letter
M6	On-the-Job Mastery & Specialization	Year 1-2 in industry	Industry Certifications
M7	Senior Track: Leading & Building	Year 3-5 in industry	Led a full engagement end-to-end

M
1

Foundation - How Everything Works

College Year 1-2 · Entry condition: none required

You cannot hack what you do not understand. Before touching a single security tool, you need a genuine mental model of how networks, operating systems, and web applications actually function. This milestone is about building that foundation.

STEP 1.1 Master Networking from First Principles

Everything in security travels across a network. This is non-negotiable knowledge.

- OSI model and TCP/IP model - understand each layer and why it matters for attacks
- IP addressing, subnetting (CIDR), routing - practice calculating subnets by hand
- DNS: how a domain resolves to an IP; how DNS hijacking works conceptually
- HTTP/S: request structure, headers, methods (GET/POST/PUT/DELETE), response codes
- Protocols to know deeply: TCP handshake, UDP, ICMP, SSH, FTP, SMTP, DHCP
- Packet analysis: install Wireshark, capture your own traffic, identify protocols



Operational action

Download Cisco Packet Tracer (free). Build a network from scratch: router, switch, two PCs, configure DHCP, watch traffic in Wireshark. Do not just watch videos - physically build it.

STEP 1.2 Linux - The Operating System of Security

Kali Linux is the industry-standard attacker OS. 90% of penetration testing happens in a terminal.

- File system hierarchy: /, /etc, /var/log, /home, /tmp - know what lives where
- Permissions: chmod, chown, SUID/SGID bits - understand privilege escalation implications
- Process management: ps, top, kill, systemctl, cron jobs
- Networking commands: ifconfig/ip, netstat/ss, nmap basics, curl, wget
- Text processing: grep, awk, sed, cut, sort, uniq - essential for log analysis
- Shell scripting: write a 20-line bash script that automates a task you do manually



Operational action

Install VirtualBox (free). Create a Kali Linux VM. Complete the 'Linux Fundamentals' module on TryHackMe (tryhackme.com) - it is free and takes 4-6 hours. Don't move on until you can navigate the file system confidently without looking up commands.

STEP 1.3 Windows & Active Directory Basics

- Windows registry: what it is, key hives (HKLM, HKCU), what attackers look for
- Event Viewer: Security, System, Application logs - identify failed login attempts
- Active Directory concepts: domains, forests, trusts, users, groups, GPOs, Kerberos authentication
- PowerShell fundamentals: running scripts, execution policy, basic commands
- Windows services and scheduled tasks - common persistence mechanisms

**Operational action**

Download a free Windows Server 2019 evaluation VM from Microsoft. Set up a basic Active Directory domain with two user accounts. Practice joining a Windows 10 VM to the domain.

STEP 1.4 Web Application Fundamentals

- HTTP in depth: how the browser sends a request, what headers mean, cookie mechanics
- HTML and JavaScript basics: enough to read source code and understand DOM manipulation
- SQL basics: SELECT, INSERT, UPDATE, DELETE - know what a query looks like
- Authentication: session tokens, cookies, JWTs - how applications remember who you are
- Browser DevTools: inspect network requests, modify cookies, view source in real time

**Operational action**

Set up DVWA (Damn Vulnerable Web Application) in your Kali VM. Browse to it in Firefox, open DevTools, and watch every HTTP request as you click around the site. This is the most important exercise of Milestone 1.

Milestone 1 - Exit Deliverable

✓	Home lab is running VirtualBox with Kali Linux VM + DVWA accessible at a local IP
✓	TryHackMe Pre-Security path complete Screenshot of completion badge saved
✓	Wireshark capture done You have captured and identified at least 5 different protocols in your own traffic
✓	Active Directory lab exists Windows Server VM with at least one domain user created
✓	Linux command fluency You can navigate, grep logs, and write a basic bash script without looking things up

CompTIA Network+ (study now)	CompTIA Security+ (target: Year 2)	Google Cybersecurity Certificate (free, 6 months)
------------------------------	------------------------------------	---

M
2

Core Skills - Offense & Defense

College Year 2-3 · Entry condition: Milestone 1 complete

With your foundation solid, you now split your learning into two tracks simultaneously - offensive and defensive. The best penetration testers understand detection; the best defenders understand attacks. Learn both.

STEP 2.1 Offensive Track - Web Application Hacking

The OWASP Top 10 [6] is your curriculum. Every category must be understood conceptually and exploited in a lab.

- Set up Burp Suite Community Edition - learn the Proxy, Repeater, and Intruder tools
- SQL Injection: manual payloads first, then SQLmap. Understand error-based, blind, and time-based techniques
- Cross-Site Scripting (XSS): reflected, stored, and DOM-based. Understand why cookies get stolen
- IDOR (Insecure Direct Object Reference): change a user ID in a request, access another user's data
- Authentication attacks: brute force with Hydra, password spraying, credential stuffing
- Directory enumeration: Gobuster and Dirsearch to find hidden paths
- File inclusion vulnerabilities: LFI and RFI - understand path traversal



Operational action

Complete ALL modules in PortSwigger Web Security Academy (portswigger.net/web-security). It is 100% free and is the single best web application security course in existence. Budget 80-100 hours.

STEP 2.2 Offensive Track - Network Penetration Testing

- Nmap: service detection (-sV), OS detection (-O), scripting engine (--script), output formats
- Metasploit Framework: understand the architecture (exploits, payloads, post modules, handlers)
- Password attacks: Hashcat for offline hash cracking, Hydra for online brute force
- Enumeration: SMB (enum4linux), FTP anonymous access, SNMP walking
- Vulnerability scanning: OpenVAS or Nessus Essentials (free) against your own lab VMs
- Privilege escalation: Linux (SUID, sudo misconfig, cron), Windows (token impersonation, unquoted service paths)



Operational action

Download 5 machines from VulnHub (vulnhub.com). Compromise each one end-to-end: scan, enumerate, exploit, escalate, document. Write 1 paragraph of notes for every machine - this is the beginning of your report-writing habit.

STEP 2.3 Defensive Track - SOC & Threat Detection

Even if you want to be an offensive specialist, understanding defensive tools makes you dramatically better at evading and simulating real attacks.

- SIEM fundamentals: install the Elastic Stack (ELK) in a VM, ship Windows logs to it, write a search query
- Log analysis: identify a brute-force attack from raw authentication logs
- MITRE ATT&CK [9]: study at least 10 techniques across Initial Access, Execution, and Persistence tactics
- Incident response: understand the 6-phase NIST IR lifecycle (Prepare → Identify → Contain → Eradicate → Recover → Post-incident)
- Blue Team Labs Online (blueteamlabs.online): complete 5 beginner investigations

**Operational action**

Download the MITRE ATT&CK Navigator (attack.mitre.org/resources/attack-navigator). Map out the techniques used in a known attack (e.g. NotPetya or WannaCry) and color-code your navigator. This exercise teaches you to think like both attacker and defender simultaneously.

STEP 2.4 Capture The Flag Competitions

CTFs are structured hacking competitions. They are the fastest way to build diverse offensive skills and the best thing you can put on a resume before your first job.

- picoCTF (picoctf.com): run by Carnegie Mellon University, completely free, beginner-friendly
- CTFtime.org: calendar of global CTF events - join at least 4 competitions per year
- HackTheBox Starting Point (free): a guided track of machines designed for absolute beginners
- After every CTF, write a writeup even if you didn't finish - explain what you tried, what worked, what didn't

**Target rank**

Reach HackTheBox 'Hacker' rank before leaving college. This requires solving ~20 machines. Post every writeup on GitHub. By graduation, this public profile is more valuable than your GPA to most security employers.

Milestone 2 - Exit Deliverable

✓	PortSwigger Academy complete Screenshot of your learning path progress showing all web modules done
✓	5 VulnHub machines rooted Notes document for each machine: scan results, exploit used, flag captured
✓	HTB Hacker rank achieved Public HTB profile URL saved

✓	First CTF participation done CTFtime profile with at least one competition listed
✓	MITRE ATT&CK navigator map A colored navigator map of a real-world attack campaign
✓	ELK lab running Windows event logs visible in Kibana dashboard

CEH (study in final year)	eJPT (affordable, hands-on exam)	TryHackMe Jr Pen Tester path
----------------------------------	---	-------------------------------------

M
3

Application Security Deep Dive

College Year 3 / Final Year · Entry: Milestone 2 complete

Web and API security is the core of most VAPT roles. This milestone takes you from 'I can follow a tutorial' to 'I can find vulnerabilities independently in an application I've never seen before.'

STEP 3.1 Advanced Web Application Testing

- Server-Side Request Forgery (SSRF): force a server to call internal endpoints, access cloud metadata.
- XML External Entities (XXE): file read via XML parsers, blind XXE via out-of-band channels
- Insecure Deserialization: understand why deserializing untrusted data leads to RCE
- Template Injection (SSTI): identify template engines, inject payloads to achieve code execution
- OAuth 2.0 attacks: state parameter bypass, redirect URI manipulation, token leakage
- JWT attacks: alg:none attack, RS256 to HS256 confusion, weak secret brute force
- Race conditions: simultaneous requests to trigger business logic flaws (e.g. use a discount twice)
- CORS misconfiguration: understand Origin reflection and how to abuse it for credential theft



Operational action

Complete the 'Advanced Topics' section of PortSwigger Academy. For every vulnerability type, replicate the attack in DVWA or a Docker-based lab (use GitHub: vulhub/vulhub for vulnerable application containers).

STEP 3.2 API Security Testing

APIs are the most under-tested attack surface in modern applications. The OWASP API Security Top 10 [13] is your guide.

- API discovery: find undocumented endpoints via JS file analysis, Google dorking, Shodan
- Authentication testing: missing auth headers, token reuse after logout, JWT weaknesses
- BOLA (Broken Object Level Authorization): change resource IDs to access other users' data
- Mass assignment: send extra fields in a POST request to escalate privileges
- GraphQL: introspection queries, batch attacks, info disclosure via verbose errors
- Tools: Postman (import OpenAPI specs), Burp Suite, ffuf for endpoint fuzzing



Operational action

Set up the crAPI (Completely Ridiculous API) vulnerable lab: github.com/OWASP/crAPI. This is the official OWASP API security practice environment. Find and exploit every vulnerability in it.

STEP 3.3 Report Writing - Your Most Underrated Skill

A penetration test that cannot be communicated is worthless. Report writing is what separates professional pentesters from hobbyist hackers.

- Executive Summary: 1 page, no technical jargon, written for a non-technical CEO - describes overall risk
- Findings section: for each vulnerability - title, CVSS score, description, proof-of-concept (screenshot + request/response), business impact, remediation steps
- CVSS v3.1 scoring [14]: learn to calculate Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, CIA impact scores
- Evidence capture: Burp Suite 'Save item', terminal screenshots with timestamps, clear filenames
- Remediation guidance: be specific - not 'fix the SQL injection' but 'use parameterized queries with PDO::prepare()'

**Operational action**

Read 5 public pentest reports (HackerOne disclosed reports, Cure53 public audits at cure53.de/pentest-advisory). Note how they structure findings. Write your first full report on your DVWA/crAPI lab - minimum 8 findings, executive summary included.

Milestone 3 - Exit Deliverable

✓	OWASP Top 10 lab - all 10 exploited For each OWASP category: one screenshot of a successful PoC in your lab
✓	crAPI fully compromised Document showing all OWASP API Top 10 found in crAPI
✓	First full pentest report written PDF report with executive summary + minimum 8 findings
✓	CVSS scoring practice 5 vulnerabilities scored in the CVSS Calculator with justification notes
✓	PortSwigger advanced labs done Screenshot of advanced labs completion page

BSCP (Burp Suite Certified - study now)**OWASP Application Security Verification Standard**

M
4

Portfolio & First Real Experience

Final Year + Graduation · Entry: Milestone 3 complete

This milestone is entirely about building public, verifiable evidence of your skills. By the end of Milestone 4, a hiring manager who has never met you should be able to spend 20 minutes reviewing your work and conclude that you can find real vulnerabilities.

STEP 4.1 Build Your Public GitHub Profile

- Create organized repositories - one for CTF writeups, one for lab notes, one for tools you've written
- Write a README for every repository: what it is, why it exists, how to use it
- Upload at least 3 Bash/Python tools you have written yourself - scanners, parsers, report generators
- Aim for consistent commits - daily or every-other-day activity shows sustained engagement
- Pin your 3 best repositories to your GitHub profile page



Why this matters

Many companies run automated GitHub analysis on applicants. A profile with 40+ commits, 3+ repos, and readable code communicates 'this person actually builds things' without a word of your CV.

STEP 4.2 Write and Publish Writeups

- Start a blog - Medium, GitHub Pages, or a personal WordPress site (free)
- Write a walkthrough for every HackTheBox machine you solve after it retires (HTB policy)
- For each writeup: explain your enumeration process, what you tried that failed, what succeeded and why
- Quality over quantity: one detailed 2,000-word writeup is worth more than ten 200-word bullet lists
- Share on LinkedIn and Twitter/X with relevant hashtags (#VAPT #HackTheBox #CTF) - build visibility



Operational action

Target 10 published writeups before applying for your first role. IppSec on YouTube shows how professionals explain their methodology - study his structure, then use your own words.

STEP 4.3 Bug Bounty - Find Your First Real Vulnerability

Bug bounty transforms you from someone who hacks practice environments into someone who has found real vulnerabilities in real production systems. Even a single low-severity finding changes how you present yourself.

- Join HackerOne (hackerone.com) [10] or Bugcrowd (bugcrowd.com) [11] - both free to join
- Start with programs that have 'Easy' difficulty tags or small-scope programs (single domain)
- Read every disclosed report in your target program before testing - understand what has already been found
- Focus on logic flaws and IDOR first - they require understanding the application, not tool expertise
- If rejected, ask for feedback - many programs give detailed triage notes
- Even a P5 informational report on your resume shows you tested a real target

**Realistic expectation**

Most beginners submit 20-40 reports before getting their first valid finding. This is normal. Each rejection teaches you something. Keep a log of everything you submitted and why it was rejected.

STEP 4.4 College-Era Opportunities

- Join or found a cybersecurity club at your college - this demonstrates leadership even before employment
- Participate in national competitions: Smart India Hackathon, C0C0N CTF, Null Humla (India); CCDC, CPTC (USA)
- Apply for security internships in your final year - even non-security internships where you can contribute to security tasks
- Attend security conferences: Null.community meetings (free, India), DEF CON (USA, affordable), BSides events
- Apply for the HackerOne Bug Bounty Hunting Scholarship or Google Summer of Code security projects
- Reach out to professionals on LinkedIn - a specific, thoughtful message asking for a 15-minute call is accepted more often than you think

Milestone 4 - Exit Deliverable

✓	GitHub profile is public and active Profile URL with 3+ pinned repos, 40+ total commits, at least 2 original tools
✓	10 published writeups Blog URL with at least 10 HTB/CTF/lab writeups published publicly
✓	First bug bounty report submitted HackerOne or Bugcrowd profile showing at least 1 submitted report (valid or not)
✓	One professional pentest report A polished PDF report on a practice environment - ready to show an interviewer
✓	LinkedIn profile complete Photo, summary, all certifications, GitHub and blog links added

M
5

Land Your First Security Role

0-6 months post-graduation · Entry: Milestone 4 complete

This milestone is about converting your skills into an offer. The VAPT job search is different from general tech hiring - your GitHub, HTB rank, and writeups matter more than your GPA or the name of your university.

STEP 5.1 Understand the Entry-Level Security Job Market

Role	What You Actually Do	Skills Most Important	Entry Path
SOC Analyst (Tier 1)	Monitor SIEM alerts, triage, escalate	Log analysis, MITRE ATT&CK, Splunk/ELK	Easiest entry - most openings
Junior Pen Tester	Assist in web/network VAPT engagements	Burp Suite, report writing, OWASP Top 10	HTB rank + sample report required
Security Analyst	Vuln mgmt, scanning, risk reporting	Nessus/Qualys, CVSS scoring, ticketing	Broad role, good stepping stone
GRC Analyst	Compliance audits, policy writing, risk assessments	ISO 27001, NIST CSF, Excel	Less technical - good if you like frameworks
Bug Bounty Hunter (freelance)	Test targets independently, write reports	Web/API skills, persistence	Not a 'job' but valid income + experience

STEP 5.2 Craft a Resume That Gets Responses

- One page maximum - no exceptions for entry-level
- Lead with: certifications, HTB/THM rank, GitHub URL, blog URL - before work experience
- For each project/lab, write: 'Identified and exploited [vulnerability type] in [environment] using [tool], resulting in [impact]'
- Skills section: list specific tools (Burp Suite, Nmap, Metasploit, Splunk, SQLmap) - not vague terms like 'cybersecurity knowledge'
- Quantify everything possible: '10 published writeups', '20 HTB machines rooted', '40+ GitHub commits'
- Use keywords from the job description verbatim - most companies use ATS resume scanning



Common resume mistake

Writing 'Knowledgeable in penetration testing and ethical hacking' says nothing. 'Identified a stored XSS vulnerability in DVWA and escalated to session hijacking, documented in a professional report following PTES methodology' says everything.

STEP 5.3 The Interview Process - What to Expect

Security interviews at entry level typically involve a combination of technical screening, practical exercises, and cultural fit assessment.

- Technical screening call: explain TCP vs UDP, HTTP vs HTTPS, what happens in a SQL injection
- Take-home challenge: common at junior pentesting firms - a small CTF machine or a vulnerable web app
- Live coding / tool demo: walk through a Burp Suite session on a practice target
- Report review: many firms ask you to explain a previous report you've written - bring your sample
- Behavioral questions: 'Tell me about a time you found something unexpected in a lab' - have 3 stories ready

**Interview preparation**

Set up a simple vulnerable lab (DVWA or a HackTheBox machine) and practice narrating your process out loud as you test it. You will often be asked to share your screen and hack live. Talking through your methodology is a skill - practice it.

STEP 5.4 Where to Find Opportunities

- LinkedIn: turn on 'Open to Work' with specific job titles (Junior Penetration Tester, SOC Analyst, Security Analyst)
- Company career pages: smaller security consultancies (Mandiant, Rapid7, NCC Group, Secureworks, Deloitte Cyber) often have entry programs
- Null.community (India): job board and community with a strong security hiring network
- EC-Council Community, ISC2 community, Cybersecurity Forum India on LinkedIn
- Direct outreach: find a senior penetration tester on LinkedIn at a target company and send a specific message - 'I have X and Y skills, I saw you are growing your VAPT team, I'd love to learn what you look for in junior hires'
- Security conferences and meetups: many entry-level hires happen through in-person community connections

Milestone 5 - Exit Deliverable

✓	Job offer signed Offer letter from a security team - any role that puts you in a security environment
✓	Resume reviewed by a practitioner At least one working security professional has given written feedback on your CV
✓	5 applications sent per week Maintained for at least 8 weeks - documented in a spreadsheet
✓	2 technical interviews completed Regardless of outcome - the practice is the goal

M
6

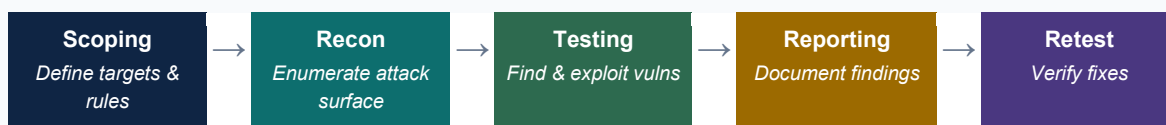
On-the-Job Mastery & Specialization

Year 1-2 in industry · Entry: First role secured

Your first 18 months in industry are the most accelerated learning period of your career. You will learn more in 3 months on the job than in 12 months of self-study. Use this milestone to build professional-grade skills and earn the OSCP.

STEP 6.1 Professional Engagement Workflow

This is how real VAPT engagements run. Learn this process from your first day.



- Scoping call: agree on IP ranges, domains, testing window, out-of-scope items, emergency contacts
- Rules of engagement (RoE): signed document before any testing begins - your legal protection
- Passive reconnaissance: WHOIS, DNS enumeration (dnsx, subfinder), Shodan, Wayback Machine
- Active reconnaissance: port scanning, service fingerprinting, web crawling
- Exploitation: follow the methodology, don't jump to Metasploit immediately - manual first
- Evidence collection: timestamp every screenshot, save every Burp request, keep a running notes log
- Retesting: after client fixes, re-execute the exact original PoC to confirm remediation

STEP 6.2 Earn the Industry Recognised Certification

The most common Offensive Security Certified Professional (OSCP) [12] is the benchmark certification for penetration testers. It is a 24-hour practical exam - you compromise machines, then write a report. There is no multiple choice. It cannot be faked.

- Prerequisites: complete HTB Hacker rank + OSCP preparation machine list (github.com/tjnull/TJNULL-OSCP)
- Enroll in PEN-200 course (OffSec): 90-day lab access included with exam attempt
- Lab strategy: do every exercise in the course modules first, then move to lab machines
- Exam format: 24 hours to compromise machines (standalone + Active Directory set), then 24 hours to write report
- Report is graded: clean, professional documentation is required even if you compromise all machines
- Study timeline: 6-9 months of consistent daily preparation after Milestone 5 skills are solid



OSCP preparation resources

OSCP guide, NetSecFocus Trophy Room, r/oscp subreddit. After every practice machine, write a full report - this trains both technical and documentation muscles simultaneously.

STEP 6.3 Choose Your Specialization

Specialization	Core Technical Skills	Key Tools	Entry Cert
Web & API Security	Advanced injection, OAuth, JWT, GraphQL, race conditions	Burp Suite Pro, ffuf, jwt_tool	BSCP
Mobile Security (Android/iOS)	APK reverse engineering, Frida hooking, SSL pinning bypass, runtime analysis	MobSF, Frida, objection, jadx	GMOB
Cloud Security (AWS/Azure/GCP)	IAM enumeration, S3 exposure, container escape, Lambda abuse	Pacu, Prowler, ScoutSuite, Trivy	AWS Security Specialty
Active Directory / Red Team	Kerberoasting, Pass-the-Hash, BloodHound, C2 frameworks, phishing	Cobalt Strike / Havoc, BloodHound, Impacket	C RTP then C RTO
DevSecOps / AppSec Engineering	SAST/DAST pipeline integration, threat modeling, secure code review	Semgrep, Snyk, OWASP ZAP, Checkov	CSSLP or GWEB

Milestone 6 - Exit Deliverable

✓	OSCP certification earned Certificate number and digital badge
✓	10 professional engagement reports written Portfolio of reports from real or detailed lab engagements
✓	Specialization chosen and active Enrolled in advanced training path for chosen domain
✓	Mentored one junior Helped a newer team member or community member through a technical challenge

OSCP (primary target)	BSCP / C RTP / AWS Security (specialization)	GPEN (optional)
------------------------------	---	------------------------

M
7

Senior Track - Leading & Building

Years 3-5 in industry · Entry: OSCP + Milestone 6 complete

At this level, technical skill is assumed. What differentiates senior professionals is the ability to plan complex engagements, communicate risk to business leaders, build and improve programs, and develop the next generation of practitioners.

STEP 7.1 Lead Full Engagements End-to-End

- Scoping calls: drive the conversation, ask the right questions, identify edge cases in scope definitions
- Proposal writing: estimate hours, define methodology, price engagements (if client-facing)
- Test plan: define attack scenarios, assign team members to workstreams, set internal milestones
- Quality review: review junior reports for technical accuracy, clarity, and completeness before delivery
- Debrief calls: present findings verbally to the client, answer technical questions from developers
- Remediation guidance: advise developers on how to fix vulnerabilities - not just what to fix but how

STEP 7.2 Threat Modeling & Architecture Review

Senior security professionals influence how software is designed - not just how it is tested after the fact.

- STRIDE model: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- PASTA (Process for Attack Simulation and Threat Analysis): business-centric threat modeling framework
- Data Flow Diagrams (DFDs): draw how data moves through a system and identify trust boundaries
- Threat modeling in the SDLC: how to run a 2-hour threat modeling session with a development team
- Secure design patterns: defense in depth, principle of least privilege, fail securely, zero trust



Required reading

Read 'Threat Modeling: Designing for Security' by Adam Shostack. It is the definitive guide to the practice and is referenced by OWASP, NIST, and Microsoft.

STEP 7.3 Give Back - Write, Speak, Teach

The security community is unusually generous with knowledge. Contributing back accelerates your own career more than any certification.

- Present at a local security meetup (Null.community, OWASP chapter meetings) - even a 15-minute talk counts

- Write for a security publication: Infosec Write-ups (Medium), NullByte, your company blog
- Release a tool on GitHub: even a small utility that solves a problem you encountered
- Mentor on platforms like ADPList.org or through your university's alumni network
- Submit a research talk to BSides or DEF CON - the submission process itself is educational even if rejected

STEP 7.4 Advanced Certifications - Choose Your Path

Certification	Focus Area	Exam Format	Who It Is For
CRT0 (Zero-Point Security)	Red team operations, C2, AD	48-hour practical lab exam	Red team operators
CRTP (Pentester Academy)	Active Directory attack chains	24-hour practical exam	AD-focused pentesters
CREST CRT / CCT	UK/APAC regulated pentesting	Written + practical	Consulting firms, regulated sectors
CISSP (ISC2)	Security management & architecture	700+ adaptive multiple choice	Moving into architecture or management
CISM (ISACA)	Security program management	150 multiple choice	Security managers and consultants

Milestone 7 - Exit Deliverable

✓	Led a full engagement solo Scoped, tested, and delivered a complete engagement report independently
✓	Threat model produced A DFD-based threat model for a real or realistic application
✓	Public talk or article delivered A recorded meetup talk or published article URL
✓	Advanced cert in progress or achieved CRT0, CRTP, CISSP, or CISM enrolled or passed
✓	Junior mentored to their first role A junior you helped can now reference you as a mentor

Complete Operational Workflow Summary

The diagram below shows the complete transaction flow of a VAPT engagement - from initial client conversation to final report delivery. Learn this process from your first day in the industry.

Phase A - Pre-Engagement

Step	Activity	Who	Output / Document
A1	Initial client inquiry and requirement gathering	Sales / Security Lead	Scoping questionnaire completed
A2	Define scope: IP ranges, domains, application URLs, exclusions	Lead Pentester + Client	Scope document (signed by both parties)
A3	Rules of Engagement: permitted techniques, testing window, emergency contacts, data handling	Legal + Security Lead	RoE document (legally signed)
A4	Threat modelling: identify high-value targets, threat actors, attack scenarios	Lead Pentester	Threat model / attack plan
A5	Environment setup: VPN access, test accounts, staging vs production confirmation	Client IT + Pentester	Test credentials + VPN config
A6	Kick-off call: confirm scope, contacts, escalation procedure, reporting format	All parties	Signed-off engagement brief

Phase B - Reconnaissance

Step	Activity	Tools	Output
B1	Passive OSINT - company structure, employee names, email formats, tech stack	LinkedIn, Hunter.io, Shodan, Google dorks	OSINT notes document
B2	DNS enumeration - subdomains, mail records, zone transfers	Subfinder, dnsx, dig, Amass	Subdomain list
B3	Web crawling and technology fingerprinting	WhatWeb, Wappalyzer, Burp Suite Spider	Technology stack map
B4	Port and service scanning (external)	Nmap, Masscan, Shodan Internetdb	Open port and service list
B5	Historical exposure review - leaked credentials, old endpoints	Wayback Machine, Grep.app, Have I Been Pwned API	Exposure report

Phase C - Active Testing

Step	Activity	Methodology	Output
C1	Authentication testing - login, password reset, MFA bypass, account lockout	OWASP Testing Guide OTG-AUTHN	Authentication findings log
C2	Authorization testing - IDOR, privilege escalation, horizontal access control	OWASP OTG-AUTHZ	Authorization findings log
C3	Input validation - injection (SQL, command, SSTI, XXE, SSRF)	OWASP OTG-INPVAL	Injection findings log
C4	Session management - token entropy, fixation, CSRF	OWASP OTG-SESS	Session findings log
C5	Business logic - race conditions, workflow bypass, pricing manipulation	Manual analysis	Logic findings log
C6	Configuration review - security headers, TLS, CORS, verbose errors, default credentials	OWASP OTG-CONFIG	Config findings log

C7	Third-party and API testing - partner integrations, webhook abuse, API key exposure	OWASP API Top 10	API findings log
----	---	------------------	------------------

Phase D - Post-Exploitation & Documentation

Step	Activity	Tool / Technique	Output
D1	Pivot and chain vulnerabilities - demonstrate realistic attack path from initial finding to maximum impact	Manual chaining, Metasploit post modules	Attack chain diagram
D2	Data exfiltration demonstration - show what data is realistically extractable (PII, credentials, source code)	Controlled demo with approval	Impact evidence screenshots
D3	Finding deduplication - consolidate related findings, remove false positives	Burp Suite issue tracker, manual review	Deduplicated findings list
D4	CVSS scoring for every finding	CVSS v3.1 calculator (first.org/cvss)	Scored findings list
D5	Evidence packaging - screenshots, HTTP requests/responses, video PoC for critical findings	Burp Suite save, ffmpeg screen capture	Evidence archive (zip)

Phase E - Reporting & Closure

Step	Activity	Standard	Output
E1	Draft report - executive summary, methodology, findings, appendices	PTES Reporting Guidelines [13]	Draft report (PDF/DOCX)
E2	Internal peer review - second pentester reviews all findings for accuracy and clarity	Internal QA process	Reviewed draft
E3	Client draft delivery - send draft for factual accuracy	Email with draft report	Client-reviewed draft

	review (not for changing risk ratings)		
E4	Final report delivery - incorporate factual corrections, deliver final signed report	Encrypted PDF delivery	Final report (signed)
E5	Debrief call - walk client through findings verbally, answer developer questions	Live call or recorded video	Meeting notes / recording
E6	Remediation tracking - client remediates findings, requests retest	Vulnerability tracker	Remediation status log
E7	Retest and closure report - verify each fix with original PoC, issue closure letter	Re-run original PoC exactly	Closure report

Essential Tools Reference

Tool	Category	Use Case	Cost
Burp Suite Community / Pro	Web app testing	Proxy, scanner, active testing - the primary VAPT tool	Free / \$499/yr
Nmap	Network scanning	Port scan, service version detection, OS fingerprint, scripting	Free
Metasploit Framework	Exploitation	Exploit modules, payloads, post-exploitation, persistence	Free (open source)
Wireshark	Packet analysis	Capture and analyze network traffic, identify protocols and attacks	Free
SQLmap	Injection testing	Automated SQL injection detection and exploitation	Free
Hydra / Medusa	Password attacks	Online brute force - HTTP, SSH, FTP, SMB, RDP	Free
Hashcat	Password cracking	Offline hash cracking with GPU acceleration	Free
Gobuster / ffuf	Directory/parameter fuzzing	Enumerate hidden paths, parameters, virtual hosts	Free
BloodHound / SharpHound	Active Directory	Map AD relationships, find attack paths to Domain Admin	Free
Impacket	Windows protocols	SMB, Kerberos, DCOM attacks - Python toolkit	Free
MobSF	Mobile security	Static and dynamic analysis of Android/iOS applications	Free
Trivy / Gype	Container security	Scan Docker images and filesystems for CVEs	Free
Subfinder / Amass	Reconnaissance	Passive and active subdomain enumeration	Free
OWASP ZAP	DAST	Automated web app scanner, good for CI/CD integration	Free
CyberChef	Data manipulation	Encode/decode/transform data - the Swiss Army knife	Free (web)

References

All URLs verified as of available resource, may change at any point of access. For academic or educational use only

- [1] ISC2 Cybersecurity Workforce Study 2023 - <https://www.isc2.org/research/workforce-study>
- [2] U.S. Bureau of Labor Statistics - Information Security Analysts - <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
- [3] TryHackMe Learning Paths - <https://tryhackme.com/paths>
- [4] HackTheBox Practice Platform - <https://www.hackthebox.com>
- [5] PortSwigger Web Security Academy (free) - <https://portswigger.net/web-security>
- [6] OWASP Top 10 - 2021 - <https://owasp.org/www-project-top-ten/>
- [7] OWASP Testing Guide v4.2 - <https://owasp.org/www-project-web-security-testing-guide/>
- [8] MITRE ATT&CK Framework - <https://attack.mitre.org>
- [9] MITRE ATT&CK Navigator - <https://mitre-attack.github.io/attack-navigator/>
- [10] HackerOne Bug Bounty Platform - <https://www.hackerone.com>
- [11] Bugcrowd Bug Bounty Platform - <https://www.bugcrowd.com>
- [12] Offensive Security OSCP - PEN-200 - <https://www.offsec.com/courses/pen-200/>
- [13] OWASP API Security Top 10 - <https://owasp.org/API-Security/editions/2023/en/0x00-header/>
- [14] CVSS v3.1 Calculator - FIRST.org - <https://www.first.org/cvss/calculator/3.1>
- [15] PTES - Penetration Testing Execution Standard - http://www.pentest-standard.org/index.php/Main_Page
- [16] VulnHub - Downloadable Vulnerable VMs - <https://www.vulnhub.com>
- [17] OWASP crAPI - Vulnerable API Practice Environment - <https://github.com/OWASP/crAPI>
- [18] TJNull OSCP Preparation Machine List - <https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yZrqQhKDtBngUHNcW8/edit>
- [19] CTFtime.org - Capture the Flag Events Calendar - <https://ctftime.org>
- [20] Blue Team Labs Online - <https://blueteamlabs.online>

"The quieter you become, the more you are able to hear."

- Kali Linux motto · and the first lesson of a security career