Module-wise Curriculum

SOC & BLUE TEAM OPERATIONS

Duration: 2 Months

Program Objective

To train learners to **detect, investigate, and respond to real-world security incidents**, with a strong understanding of attacker behavior and defender trade-offs.

Module 1: Understanding Attacker Behavior

Focus: How attacks look from a defender's perspective

- Common attacker objectives and workflows
- Kill chain and attacker lifecycle (practical view)
- Mapping attacker actions to observable signals
- Why most attacks go unnoticed initially

Outcome:
Learners understand *what matters* to attackers and what defenders should actually watch for.

Module 2: Visibility, Logs & Telemetry

Focus: What data matters — and what doesn't

- Log sources across systems and applications
- Endpoint, network, and application telemetry
- Common visibility gaps in real environments

- Noise vs signal in security data

Outcome:
Learners can identify meaningful telemetry and avoid alert fatigue.

Module 3: Detection & Alerting

Focus: Identifying suspicious behavior reliably

- Detection logic fundamentals
- Behavior-based vs signature-based detection
- Alert triage and prioritization
- False positives and tuning realities

Outcome:
Learners learn to treat alerts as *starting points*, not conclusions.

Module 4: Investigation & Analysis

Focus: Making sense of an incident

- Incident scoping and timeline reconstruction
- Correlating events across multiple sources
- Root cause analysis
- Evidence handling and documentation

Outcome:
Learners can reconstruct incidents and understand *how and why* they happened.

Module 5: Response & Containment

Focus: Acting under pressure

- Incident response workflows
- Containment strategies and trade-offs
- Coordination with engineering and stakeholders
- When to contain, isolate, or observe

Outcome:
Learners can respond decisively without causing unnecessary damage.

Module 6: Post-Incident Learning & Improvement

Focus: Getting better after failure

- Lessons learned and retrospective analysis
- Improving detections based on real incidents
- Closing gaps attackers exploited
- Building feedback loops between offense and defense

Outcome:
Learners understand how mature security teams evolve over time.

ETHICAL HACKING

Duration: 3 Months

Program Objective

To build **strong offensive security foundations** by teaching learners how attackers discover, exploit, and move through real systems — responsibly and methodically.

Module 1: Attacker Foundations

Focus: Thinking like an attacker, not a tool operator

- Attacker goals and motivation
- Networking fundamentals from an attacker's perspective
- Linux fundamentals for offensive operations
- Understanding trust boundaries and assumptions

Outcome:
Learners begin thinking in terms of *systems and weaknesses*, not commands.

Module 2: Reconnaissance & Enumeration

Focus: Finding what matters before attacking

- Asset discovery and attack surface mapping
- Service and technology fingerprinting
- Identifying high-value targets
- Common reconnaissance mistakes

Outcome:
Learners can identify realistic entry points instead of scanning blindly.

Module 3: Web Application Attack Fundamentals

Focus: Exploiting logic, not just bugs

- Authentication and authorization failures
- Input validation and injection flaws
- Session handling weaknesses
- Business logic abuse

Outcome:
Learners understand *why* web applications fail, not just how.

Module 4: Initial Access & Exploitation

Focus: Turning weaknesses into access

- Exploiting misconfigurations
- Chaining simple issues into impact
- Safe and responsible exploitation practices
- Avoiding unnecessary noise

Outcome:
Learners can gain access methodically and responsibly.

Module 5: Privilege Escalation & Lateral Thinking

Focus: Expanding control after entry

- Common privilege escalation patterns

- Credential abuse and trust exploitation
- Lateral movement concepts
- Thinking beyond single-host compromise

Outcome:
Learners understand how attackers expand reach inside systems.

Module 6: Impact, Reporting & Ethics

Focus: Acting professionally

- Demonstrating impact responsibly
- Understanding limits and boundaries
- Writing clear, useful findings
- Ethics and responsible disclosure

Outcome:
Learners learn to think like professionals, not hobbyists.

VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

Duration: 3 Months

Program Objective

To train learners to **systematically identify, validate, and communicate security risks** across systems and applications, while distinguishing real risk from noise.

This program focuses on **methodology, discipline, and judgment**, not tool-driven scanning.

Module 1: VAPT Foundations & Scope Definition

Focus: Understanding what VAPT is — and what it is not

- Difference between vulnerability assessment and penetration testing
- Common misconceptions about VAPT
- Defining scope, assumptions, and constraints
- Legal, ethical, and authorization boundaries

Outcome:
Learners understand how to approach VAPT professionally and responsibly.

Module 2: Asset Discovery & Attack Surface Mapping

Focus: Knowing what you are actually testing

- Identifying in-scope assets and services

- Understanding system architecture at a high level
- Mapping attack surfaces across applications and infrastructure
- Common blind spots in asset discovery

Outcome:
Learners can create a realistic and complete view of the target environment.

Module 3: Vulnerability Identification

Focus: Finding weaknesses without drowning in noise

- Common vulnerability classes (application, infrastructure, configuration)
- Understanding root causes vs symptoms
- Manual validation vs automated discovery
- Recognizing false positives and low-value findings

Outcome:
Learners learn to focus on vulnerabilities that actually matter.

Module 4: Validation & Responsible Exploitation

Focus: Separating theoretical issues from real risk

- Validating vulnerabilities safely
- Demonstrating exploitability responsibly
- Understanding impact without overstepping scope

- Avoiding unnecessary disruption

Outcome:
Learners can confirm real risk while maintaining professionalism.

Module 5: Risk Assessment & Prioritization

Focus: Translating findings into actionable risk

- Assessing severity beyond CVSS scores
- Understanding business impact
- Chaining vulnerabilities to show realistic attack paths
- Prioritizing fixes based on risk, not volume

Outcome:
Learners learn to think beyond “number of vulnerabilities”.

Module 6: Reporting & Communication

Focus: Making findings useful

- Writing clear and structured VAPT reports
- Explaining technical risk to non-technical stakeholders
- Providing actionable remediation guidance
- Avoiding fear-driven or inflated reporting

Outcome:
Learners can communicate risk clearly and credibly.

Module 7: Review, Retesting & Continuous Improvement

Focus: Closing the loop

- Retesting and validation after fixes
- Understanding how remediation changes risk
- Improving testing methodology over time
- Learning from previous assessments

Outcome:
Learners understand VAPT as an iterative, improving process.

ETHICAL HACKING + VAPT

Duration: 4 Months

Program Objective

To provide learners with **end-to-end offensive security capability** — from understanding attack surfaces and exploitation, to structured vulnerability assessment, validation, and professional risk communication.

This track is designed for learners who want **depth, not shortcuts**.

Module 1: Offensive Security Foundations

Focus: Building the attacker mindset

- Attacker goals, motivations, and constraints
- Networking fundamentals from an attacker's perspective
- Linux fundamentals for offensive operations
- Understanding trust boundaries and implicit assumptions

Outcome:
Learners develop a systems-level view of how attacks begin.

Module 2: Reconnaissance & Attack Surface Mapping

Focus: Knowing where to attack — and why

- Asset discovery and enumeration
- Service and technology fingerprinting
- Mapping external and internal attack surfaces
- Identifying high-value and high-risk entry points

Outcome:
Learners can identify realistic targets instead of scanning blindly.

Module 3: Vulnerability Identification & Analysis

Focus: Finding weaknesses that actually matter

- Common vulnerability classes (application, infrastructure, configuration)
- Root cause analysis vs surface symptoms
- Manual validation techniques
- Avoiding false positives and low-impact findings

Outcome:
Learners learn to separate signal from noise.

Module 4: Exploitation & Initial Access

Focus: Turning vulnerabilities into access responsibly

- Exploiting misconfigurations and logic flaws
- Safe exploitation practices
- Chaining simple issues into meaningful access
- Minimizing noise and impact

Outcome:
Learners can demonstrate real risk without reckless behavior.

Module 5: Privilege Escalation & Attack Path Development

Focus: Expanding control and impact

- Common privilege escalation patterns
- Credential abuse and trust exploitation
- Lateral movement concepts
- Building realistic attack paths

Outcome:
Learners understand how attackers expand reach within environments.

Module 6: Risk Assessment & Prioritization

Focus: Translating technical findings into risk

- Assessing severity beyond vulnerability scores
- Understanding business and operational impact
- Prioritizing vulnerabilities based on exploitability and exposure
- Avoiding vulnerability-count thinking

Outcome:
Learners can reason about risk, not just findings.

Module 7: Reporting & Professional Communication

Focus: Acting like a security professional

- Writing clear, structured VAPT reports
- Explaining risk to technical and non-technical stakeholders
- Providing actionable remediation guidance

- Ethical boundaries and responsible disclosure

Outcome:
Learners communicate findings credibly and responsibly.

Module 8: Review, Retesting & Continuous Improvement

Focus: Closing the loop

- Retesting after fixes
- Understanding how remediation changes risk
- Improving testing methodology over time
- Learning from past engagements

Outcome:
Learners understand offensive security as an iterative discipline.

OFFENSIVE & DEFENSIVE OPERATIONS (ATTACK–DETECT–RESPOND)

Duration: 4 Months

(EH + SOC + VAPT integrated track)

Program Objective

To train learners to **execute attacks, detect those attacks, investigate their impact, and respond effectively**, building a complete mental model of how real security failures occur and how mature teams operate across offense and defense.

This program focuses on **cause-and-effect learning**:

- How attacker actions create defender signals
- How defensive gaps enable deeper compromise
- How offensive insights improve detection and response

This is not a tool rotation or a simulated purple-team exercise.
It is a **systems-level understanding of security operations**.

Module 1: Attacker & Defender Mental Models

Focus: Understanding both sides before touching tools

- Attacker objectives, constraints, and trade-offs
- Defender priorities, blind spots, and operational realities
- Why attackers succeed even in “secure” environments
- How offensive and defensive teams miscommunicate

Outcome:
Learners understand **why offense and defense often fail to align**, and what each side actually needs from the other.

Module 2: Attack Surface, Visibility & Exposure

Focus: What attackers see vs what defenders see

- Attack surface mapping (external and internal)
- Visibility gaps across endpoints, networks, and applications
- What attackers exploit that defenders rarely monitor
- Where logs exist but fail to tell the full story

Outcome:
Learners can identify **mismatches between attack paths and defensive visibility**.

Module 3: Initial Access & Detection Signals

Focus: Entry points and early warning opportunities

- Common initial access vectors (misconfigurations, weak controls, logic flaws)
- Observable signals generated during early-stage attacks
- Why most early-stage activity is ignored or misclassified
- Detection trade-offs: sensitivity vs noise

Outcome:
Learners can **map attacker actions directly to detection opportunities**.

Module 4: Exploitation, Privilege Escalation & Investigation

Focus: Understanding impact through both lenses

- Exploitation patterns and privilege escalation logic
- What escalation looks like in logs and telemetry

- Correlating attacker behavior across systems
- Reconstructing timelines from incomplete data

Outcome:
Learners learn to **rebuild attacks after they happen**, not just execute them.

Module 5: Attack Path Development & Defensive Failure Analysis

Focus: Chains, not isolated issues

- Building realistic multi-step attack paths
- Identifying where controls failed or were bypassed
- Understanding compounding weaknesses
- Why “patched” systems still get compromised

Outcome:
Learners think in **paths and failure chains**, not vulnerabilities or alerts.

Module 6: Incident Response & Containment Decisions

Focus: Acting under uncertainty

- When to contain, isolate, or observe
- Trade-offs between business impact and security risk
- Coordination between SOC, engineering, and leadership
- Common response mistakes that worsen incidents

Outcome:
Learners can **make defensible response decisions**, not reflexive ones.

Module 7: Risk Communication & Reporting (Offense + Defense)

Focus: Making security findings usable

- Translating attack paths into business risk
- Writing reports that both attackers and defenders respect
- Communicating uncertainty honestly
- Avoiding fear-driven or tool-centric reporting

Outcome:
Learners communicate **risk, not noise**, to technical and non-technical audiences.

Module 8: Post-Incident Learning & Capability Improvement

Focus: Security as an evolving discipline

- Lessons learned from offensive and defensive failures
- Improving detections using real attack behavior
- Adjusting testing methodology based on defensive insight
- Building long-term feedback loops

Outcome:
Learners understand **how mature security teams improve over time**.