

DevSecOps, Infrastructure Security, Virtualization and Secure Automation on Ubuntu

Duration: 5 Days (8 Hrs./Day)

Net Instructional Time: 6 Hours per Day

Course Objective: This course provides foundational-to-intermediate knowledge of DevSecOps, secure automation, infrastructure security, CI/CD pipeline security, multi-stack build tooling, automated testing, security scanning, containerisation, Kubernetes overview, secrets management, web and application server security, database security, Ubuntu virtualization, and LLM application security. The course is designed for 30 net instructional hours, so selected topics will be covered as hands-on labs while broader platform/tooling topics will be covered as overview or guided demonstrations.

Lab Requirement: Koenig-DC/Ubuntu 24.04

Day 1: DevSecOps Foundations and Ubuntu-Based CI/CD Environment

Net Duration: 6 Hours

Module 1: Introduction to DevSecOps

Coverage Type: Overview

Estimated Time: 1 Hour

Topics

- DevOps vs DevSecOps security aspects
- Security responsibilities across development and operations
- DevSecOps lifecycle overview
- Security checkpoints in CI/CD pipelines
- Shift-left security concepts
- Common security gaps in DevOps workflows
- Secure software delivery overview

Lab / Demo

- No full lab.
- Short instructor-led discussion: mapping security checks to CI/CD stages.

Module 2: Ubuntu Lab Environment, Git Workflow, and Multi-Stack Build Tooling

Coverage Type: Overview + Guided Demo

Estimated Time: 2 Hours

Topics

- Ubuntu lab environment overview
- Linux terminal and package management overview
- Required tools and utilities overview
- Git repository workflow overview
- Build automation overview
- Java build tools:
 - Maven overview
 - Gradle overview
- Node.js build tools:
 - npm overview
 - Yarn overview
- .NET build tools:
 - dotnet CLI overview
 - MSBuild overview
- Build artifacts and dependency files across different stacks
- Dependency management and build reproducibility considerations
- Build-tool relevance in DevSecOps pipelines

Lab / Guided Demo

Guided Demo: Multi-stack build tool comparison

- Show typical Java build flow using Maven or Gradle.
- Show typical Node.js package/build flow using npm or Yarn.
- Show typical .NET build flow using dotnet CLI.
- Discuss where these commands fit inside Jenkins pipeline stages.

Module 3: CI/CD Pipeline Basics with Build Tool Integration

Coverage Type: Lab / Guided Hands-on

Estimated Time: 2.5 Hours

Topics

- Jenkins introduction
- Jenkins plugin overview
- Jenkins Pipeline structure
- Pipeline stages and execution flow
- Build stage design for different technology stacks
- Maven/Gradle build stage concept
- npm/Yarn build stage concept
- dotnet CLI/MSBuild build stage concept
- Pipeline logs and failure analysis
- Build validation overview
- Pipeline failure handling
- Quality checks before security gates

Lab: Basic Jenkins Pipeline with Build Stage

Learners will:

- Review a sample Jenkins pipeline structure.

- Identify pipeline stages such as checkout, build, test, scan, and package.
- Add or review a build stage for one selected technology stack.
- Observe pipeline logs and basic failure points.
- Discuss how build failures affect DevSecOps flow.

Day 1 Review and Q&A

Coverage Type: Review

Estimated Time: 0.5 Hour

Day 2: Automated Testing Tools and Security Testing Automation

Net Duration: 6 Hours

Module 4: Automated Testing in DevSecOps

Coverage Type: Overview + Discussion

Estimated Time: 1.25 Hours

Topics

- Purpose of automated testing in DevSecOps
- Unit testing overview
- Code coverage overview
- Build verification testing
- Regression testing overview
- Test reporting in pipelines
- Quality checks before security gates

Lab / Demo

- No separate full lab.
- Discussion-based walkthrough of where automated testing fits into CI/CD.

Module 5: Code Quality and Static Security Checks

Coverage Type: Lab / Guided Demo

Estimated Time: 2 Hours

Topics

- Static code analysis overview
- Code quality gates
- Security rules in code analysis
- Dependency vulnerability scanning overview
- Software Composition Analysis overview
- Secrets detection overview
- Handling failed quality and security checks

Lab: Static Security and Dependency Check Review

Learners will:

- Review a sample pipeline security-check stage.
- Understand how SAST/SCA/secrets-detection results are interpreted.
- Identify failed quality/security gates.
- Discuss remediation workflow after failed checks.

Module 6: Dynamic Security Testing Automation

Coverage Type: Lab / Guided Demo

Estimated Time: 2 Hours

Topics

- DAST concepts
- OWASP ZAP overview
- Passive scanning overview
- Active scanning overview
- Baseline scan concept
- Security scan reports
- Automated security testing in CI/CD pipelines

Lab: OWASP ZAP Baseline Scan Walkthrough

Learners will:

- Understand passive vs active scanning.
- Review how a baseline scan works.
- Examine a sample ZAP report.
- Identify common findings and risk levels.
- Discuss how ZAP can be integrated into CI/CD.

Day 2 Review and Q&A

Coverage Type: Review

Estimated Time: 0.75 Hour

Day 3: Containers, Kubernetes, Secrets Management, and Web/Application Server Security

Net Duration: 6 Hours

Module 7: Containerisation Overview

Coverage Type: Overview + Guided Demo

Estimated Time: 1.5 Hours

Topics

- Containerisation overview
- Docker basics
- Docker images and containers
- Dockerfile overview
- Container lifecycle overview
- Container networking overview
- Container security fundamentals
- Image scanning overview
- Secure handling of environment variables

Lab / Guided Demo

Guided Demo: Docker Build and Container Security Review

Learners will:

- Review a Dockerfile.
- Understand image vs container.
- Observe basic container lifecycle commands.
- Discuss image scanning and environment-variable risks.

Module 8: Kubernetes Overview

Coverage Type: Overview

Estimated Time: 1.25 Hours

Topics

- Kubernetes overview
- Kubernetes Pods overview

- Kubernetes Deployments overview
- Kubernetes Services overview
- Kubernetes ConfigMaps and Secrets overview
- Kubernetes security concepts overview

Lab / Demo

- No full Kubernetes lab.
- Instructor-led YAML/resource walkthrough only.

Module 9: HashiCorp Vault and Secrets Management Overview

Coverage Type: Overview + Guided Demo

Estimated Time: 1 Hour

Topics

- HashiCorp Vault overview
- Secrets management concepts
- Vault use cases overview
- Secure secrets handling in applications and pipelines
- Difference between environment variables, CI/CD secrets, Kubernetes Secrets, and Vault

Lab / Guided Demo

Guided Demo: Secrets Handling Review

Learners will:

- Review insecure vs secure secrets-handling examples.
- Understand where secrets should not be stored.
- Map secrets usage across application, pipeline, and runtime layers.

Module 10: Web Servers, Application Servers, and Reverse Proxy Security

Coverage Type: Overview + Lab

Estimated Time: 1.75 Hours

Topics

- Web server vs application server
- Reverse proxy architecture
- NGINX reverse proxy overview
- Apache HTTP Server overview
- Apache Tomcat as Java application server
- IIS as .NET hosting platform
- Request forwarding concepts
- Upstream services overview
- Host-based routing overview
- Path-based routing overview
- Load balancing overview
- TLS and HTTPS overview
- Security headers overview
- Access logging and error logging overview
- Basic hardening concepts

Lab: NGINX Reverse Proxy and Server Security Review

Learners will:

- Review a basic NGINX reverse proxy configuration.
- Understand upstream service routing.
- Review headers, logging, and TLS-related configuration points.
- Compare NGINX with Apache HTTP Server at a high level.
- Discuss where Tomcat and IIS fit in application-hosting architecture.

Coverage notes

- **NGINX:** Lab/demo focus.
- **Apache HTTP Server:** Overview/comparison only.

- **Apache Tomcat:** Overview/application-server positioning only.
- **IIS:** Overview/comparison only, because the lab environment is Ubuntu-based while IIS hosting is Windows/IIS-oriented.

Day 3 Review and Q&A

Coverage Type: Review

Estimated Time: 0.5 Hour

Day 4: Database Security and Secure Application Connectivity

Net Duration: 6 Hours

Module 11: Database Security Fundamentals

Coverage Type: Overview + Discussion

Estimated Time: 1.75 Hours

Topics

- Database security fundamentals
- Common database security risks
- Database isolation concepts
- Localhost binding and network exposure
- Firewall-based database access restriction
- Secure database authentication
- Database account management
- Least privilege access
- Role-based access overview
- Avoiding shared privileged accounts

Lab / Demo

- Scenario-based discussion.
- No full database installation lab.

Module 12: Secure Database Connectivity

Coverage Type: Guided Demo / Configuration Review

Estimated Time: 1.75 Hours

Topics

- Encrypted database connections overview
- TLS for database traffic
- Application-to-database connection security
- Secure storage of database credentials
- Secrets handling for database connectivity
- Database configuration hardening overview
- Secure backup considerations
- Database logging and auditing overview

Lab: Secure Database Connectivity Review

Learners will:

- Review secure vs insecure database connection patterns.
- Identify risks in exposed database endpoints.
- Review safe credential handling patterns.
- Discuss TLS, firewall rules, and least-privilege access.

Module 13: Database Security in DevSecOps Pipelines

Coverage Type: Lab / Checklist-Based Exercise

Estimated Time: 1.75 Hours

Topics

- Database checks in deployment workflows
- Configuration validation overview
- Dependency and migration security considerations
- Protecting database credentials in CI/CD
- Secure environment variable usage
- Database rollback and backup planning overview
- Database security review checklist

Lab: Database Security Review Checklist

Learners will:

- Apply a database security checklist to a sample deployment scenario.
- Identify weak credential handling.
- Identify missing backup/rollback considerations.
- Map database checks into CI/CD workflow stages.

Day 4 Review and Q&A

Coverage Type: Review

Estimated Time: 0.75 Hour

Day 5: Ubuntu Virtualization, LLM Application Security, and Integrated Review

Net Duration: 6 Hours

Module 14: VM Virtualization Management on Ubuntu

Coverage Type: Overview + Guided Demo

Estimated Time: 2 Hours

Topics

- Virtualization concepts
- VM vs container overview
- Hypervisor overview
- KVM overview
- libvirt overview
- Ubuntu virtualization overview
- Hardware virtualization considerations
- VM lifecycle management overview
- VM creation concepts
- Start, stop, restart, and delete VM operations
- Virtual disk overview
- VM resource allocation overview
- Virtual networking overview
- NAT and bridge networking concepts
- VM access and administration overview
- VM security considerations

Lab / Guided Demo

Guided Demo: Ubuntu Virtualization and VM Security Review

Learners will:

- Understand KVM/libvirt role in Ubuntu virtualization.
- Review VM lifecycle operations conceptually.
- Discuss NAT vs bridge networking.
- Review VM hardening considerations.

Module 15: Securing LLM Applications

Coverage Type: Overview + Scenario Discussion

Estimated Time: 1.5 Hours

Topics

- LLM application security introduction
- OWASP LLM Top 10 overview
- Prompt injection overview
- Sensitive information disclosure in LLM applications
- Insecure output handling overview
- Excessive agency overview
- Plugin and tool integration risks overview
- Data exposure risks in prompts and responses
- Access control for LLM-based applications
- Logging and monitoring considerations
- Secure LLM usage checklist

Lab / Exercise

Scenario Exercise: LLM Application Security Review

Learners will:

- Review an LLM-based application scenario.
- Identify prompt injection risks.
- Identify sensitive information disclosure risks.
- Discuss access control, logging, and safe tool integration.

Module 16: Final Integrated DevSecOps Security Review

Coverage Type: Lab / Capstone Review

Estimated Time: 1.5 Hours

Topics

- Review of DevSecOps pipeline security
- Review of build tools across Java, Node.js, and .NET projects
- Review of automated testing tools

- Review of containerisation, Kubernetes, and Vault overview topics
- Review of web servers, application servers, and reverse proxy security
- Review of database security
- Review of Ubuntu virtualization security
- Review of LLM application security
- Final integrated security scenario

Lab: Integrated DevSecOps Security Review Scenario

Learners will:

- Review a sample end-to-end application delivery flow.
- Identify where build, test, scan, package, deploy, and review stages fit.
- Map security controls across CI/CD, application server, reverse proxy, database, secrets, VM, and LLM layers.
- Produce a final security-review checklist.

Final Q&A and Best Practices Discussion

Coverage Type: Review

Estimated Time: 1 Hour

Coverage Summary: Overview vs Labs

Covered with Labs / Guided Demos

- Jenkins pipeline and build-stage review
- Multi-stack build-tool invocation overview
- Static security and dependency check review
- OWASP ZAP baseline scan walkthrough
- Dockerfile/container security review
- Secrets-handling review
- NGINX reverse proxy configuration review
- Secure database connectivity review

- Database security checklist exercise
- Ubuntu virtualization and VM security review
- LLM application security scenario
- Final integrated DevSecOps security review

Covered as Overview Only

- Full Maven implementation
- Full Gradle implementation
- Full npm/Yarn package-management deep dive
- Full dotnet CLI/MSBuild implementation
- Full Kubernetes implementation
- Full HashiCorp Vault administration
- Full Apache HTTP Server administration
- Full Apache Tomcat deployment administration
- IIS hands-on hosting
- Full database platform administration
- Full LLM security engineering implementation