

**Mastering Docker Security — Course Content**

**Module 1 – Introduction to Docker Security**

* Understanding Docker architecture
* Containers vs. virtual machines security model
* Attack surface in containerized environments
* Common Docker security incidents

**Module 2 – Docker Installation & Secure Setup**

* Installing Docker securely on Linux & Windows
* Configuring Docker daemon securely
* Docker rootless mode
* Managing users & permissions

**Module 3 – Docker Architecture & Security Components**

* Docker daemon, client, registry, and container internals
* Namespaces, cgroups, capabilities
* Storage drivers & networking in Docker

**Module 4 – Docker Threat Landscape**

* Types of attacks (container escape, privilege escalation, image poisoning)
* Common misconfigurations
* Mapping threats to MITRE ATT&CK

**Module 5 – Secure Docker Images**

* Building minimal images (distroless, Alpine)
* Removing unnecessary packages and binaries
* Vulnerability scanning with tools (Trivy, Grype, Anchore)
* Image signing & verification with Docker Content Trust

**Module 6 – Docker Registry Security**

* Securing private registries
* Registry authentication & authorization
* Image push/pull restrictions
* Protecting against malicious images

**Module 7 – Container Runtime Security**

* Dropping unnecessary Linux capabilities
* Running containers as non-root users
* Applying seccomp, AppArmor, SELinux profiles
* Controlling container privileges

**Module 8 – Docker Networking Security**

* Docker network modes & their risks
* Isolating containers with custom networks
* Preventing network sniffing & spoofing
* Firewall rules for container traffic

**Module 9 – Secrets Management in Docker**

* Securely storing and injecting secrets
* Docker secrets API
* Avoiding hardcoded credentials in images

**Module 10 – Monitoring & Logging for Docker**

* Docker logging drivers & configurations
* Centralized logging (ELK, Loki)
* Monitoring with tools like Prometheus & Grafana

**Module 11 – Vulnerability Assessment for Docker**

* Scanning containers during build & runtime
* Continuous vulnerability management
* Automating security scans in CI/CD pipelines

**Module 12 – Container Escape & Exploitation**

* Exploiting misconfigured containers
* Breaking out to the host system
* Kernel exploits via containers
* Mitigation techniques

**Module 13 – Docker in CI/CD Security**

* Securing build pipelines
* Preventing supply chain attacks
* Integrating Docker security in DevSecOps workflows

**Module 14 – Orchestrator Security (Docker Swarm)**

* Securing swarm clusters
* Role-based access control (RBAC) in Swarm
* Protecting swarm secrets & communication channels

**Module 15 – Third-Party Integrations & Risks**

* Security risks from external plugins
* Managing API integrations securely
* Validating third-party images

**Module 16 – Compliance & Audit in Docker**

* Docker audit logs
* Compliance with CIS Docker Benchmark
* Evidence collection for investigations

**Module 17 – Incident Response in Docker Environments**

* Detecting container compromise
* Isolating affected containers
* Forensics on containerized workloads

**Module 18 – Advanced Hardening Techniques**

* Immutable container patterns
* Read-only file systems
* Limiting resource usage for security

**Module 19 – Docker Security Best Practices**

* Golden rules for secure Docker deployments
* Continuous security testing
* Real-world secure deployment case studies

**Module 20 – Final Docker Security Project**

* Full containerized environment security assessment
* Exploit & harden containers in lab scenarios
* Final report & recommendations presentation