OWASP NETTACKER TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Nettacker

- Overview of OWASP Nettacker
- Nettacker vs traditional scanners (Nmap, Nessus, OpenVAS)
- Use cases: reconnaissance, vulnerability discovery, hardening validation
- Ethical hacking & legal considerations

Nettacker Architecture & Workflow

- Nettacker components and modules
- Scanning engine and plugin system
- Payloads, templates, and modules
- Understanding scan lifecycle

Installation & Environment Setup

- Installing Nettacker (Linux-based setup)

- Python environment and dependencies
- Configuration files and options
- Running Nettacker in lab environments

Target Discovery & Reconnaissance

- Host discovery and IP range scanning
- DNS, subdomain, and service discovery
- Network and infrastructure reconnaissance
- Hands-on: Run basic recon scans

Vulnerability Scanning & Module Usage

- Service-based vulnerability detection
- Web application scanning modules
- Credential checks and brute-force protections
- Understanding scan outputs

DAY 2

Web Application & API Security Scanning

- Scanning web services and APIs
- Detecting common OWASP Top 10 issues
- Authentication handling
- Rate limiting and safe scanning practices

Custom Modules & Extending Nettacker

- Creating custom scan modules

- Writing payloads and plugins
- Integrating new checks
- Best practices for custom development

Scan Optimization & Performance Tuning

- Managing large scan scopes
- Threading and performance tuning
- Reducing false positives
- Safe scanning in production-like environments

Reporting, Evidence & Risk Communication

- Understanding Nettacker reports
- Exporting results (JSON, HTML, CLI output)
- Risk scoring and prioritization
- Communicating findings to stakeholders

Nettacker in CI/CD & DevSecOps

- Using Nettacker for continuous security testing
- Integrating with pipelines
- Infrastructure-as-Code security validation
- Shift-left and shift-right strategies

Nettacker vs Other Security Tools

- Comparison with Nmap, Nikto, Burp, Metasploit
- When to combine tools
- Strengths and limitations

- Open-source security tooling strategy

Real-World Use Cases & Best Practices

- Enterprise deployment scenarios
- Common mistakes and lessons learned
- Responsible disclosure and remediation workflows
- Nettacker roadmap and community resources