OWASP AMASS TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Amass

- Overview of OWASP Amass framework
- Role of attack surface mapping in cybersecurity
- Use cases in penetration testing and red teaming
- Passive vs active reconnaissance
- Legal and ethical considerations

Environment Setup and Configuration

- Installing OWASP Amass on Linux and Windows
- Configuring API keys and data sources
- Understanding Amass configuration files
- Managing resolvers and wordlists
- Best practices for efficient scanning

Amass Architecture and Workflow

- Internal architecture of Amass
- Enumeration pipeline overview
- Data collection methods
- Handling large-scale environments
- Data storage and output management

Passive Enumeration Techniques

- Using public and third-party data sources
- Certificate Transparency log analysis
- WHOIS and ASN discovery
- Reverse DNS mapping
- Extracting domains and infrastructure

Active Enumeration Techniques

- DNS probing and validation
- Subdomain brute forcing
- Permutation generation
- Zone transfer testing
- Managing false positives

Result Analysis and Visualization

- Output formats (TXT, JSON, Graph)
- Using Amass database
- Relationship mapping
- Asset categorization

- Reporting fundamentals

Hands-on Labs

- Tool installation and setup lab
- Passive recon lab
- Active enumeration lab
- Result review exercise

DAY 2

Advanced Enumeration Strategies

- Hybrid passive and active recon
- ASN and IP range discovery
- Infrastructure and network mapping
- Cloud and SaaS asset discovery
- Shadow IT identification

Automation with OWASP Amass

- Running Amass in scripts and pipelines
- Scheduling recurring scans
- Integrating with CI/CD pipelines
- Continuous attack surface monitoring
- Managing scan output

Integration with Security Tools

- Using Amass with Nmap

- Feeding results into Burp Suite
- Exporting to vulnerability scanners
- Recon workflow automation
- Building recon frameworks

Threat Modeling Using Amass Data

- Building attack surface maps
- Prioritizing discovered assets
- Risk-based asset ranking
- Exposure analysis
- Executive reporting techniques

Performance Optimization and Evasion

- Resolver tuning
- Rate limit management
- Scan speed optimization
- Avoiding detection and blocking
- Data source reliability

Real-World Use Cases

- Bug bounty reconnaissance workflows
- Enterprise security monitoring
- Red team engagements
- Incident response support
- Continuous asset discovery

Hands-on Labs

- Advanced enumeration lab
- Automation pipeline lab
- Integration lab
- End-to-end recon project

Wrap-up and Q&A

- Key takeaways
- Best practices checklist
- Common mistakes
- Next steps for learners