CWL
CyberWarFare Labs

Commit → Build → Pwn :
Offensive Tradecraft for CI/CD Pipelines

Module 0: Introduction to DevOps

- 0.1 Software Development 101
- 0.2 Software Development Life Cycle (SDLC) Model
- 0.3 Introduction to CI/CD
- 0.4 Introduction to IaC
- 0.5 DevOps Components
  - 0.5.1 Source Code Repository
  - 0.5.2 Build
  - 0.5.3 Artifacts
  - 0..5.4 Artifact Storage
  - 0.5.5 Virtual Machines
  - 0.5.6 Containers
- 0.6 CI/CD Platforms

Module 1: Attacking Source Code Phase

1.1 Source Code Phase
1.2 GitHub 101
1.3 Demo 01: GitHub Enumeration
1.4 Backdoors 101
1.5 Demo 02: Malicious IDE Extension
1.6 Demo 03: Malicious GitHub Actions
1.7 Demo 04: NPM Package Backdoors
1.8 Takeaways

Module 2: Attacking Jenkins

- 2.1 Introduction to Jenkins
  - 2.1.1 Architecture
  - 2.1.2 Roles
  - 2.1.3 3rd-party Integrations
- 2.2 Demo 01: Cred Exfil via Misconfigured Jenkins GUI
- 2.3 Demo 02: Exfiltrating Credentials via Webhook
- 2.4 Demo 03: Pipeline Secret Access via Exposed API Token
- 2.5 Demo 04: Docker Hub Enumeration
- 2.6 Demo 05: Docker Image Poisoning
- 2.7 Demo 06: Command Execution via Jenkins Build Modification

Module 3: Attacking AWS CodePipeline

- 3.1 Introduction to AWS CodePipeline
  - 3.1.1 Architecture
  - 3.1.2 Components
  - 3.1.3 IAM Roles & Policies
  - 3.1.4 3rd-party Integrations via AWS Marketplace
- 3.2 Build Specifications
- 3.3 Attack Flow for AWS CodePipeline
- 3.4 Demo 01: Environment Variables Exfiltration
- 3.5 Demo 02: ECR Enumeration
- 3.6 Demo 03: CodeBuild Exploitation
- 3.7 Demo 04: ECS Token Exfiltration
- 3.8 Takeaways

Module 4: Attacking Azure DevOps

- 4.1 Introduction to Azure DevOps
  - 4.1.1 Basics
  - 4.1.2 Components
  - 4.1.3 Organization & Project
  - 4.1.4 Authentication
  - 4.1.5 REST API
  - 4.1.6 Pipelines
- 4.2 Basics of Entra ID & Azure Cloud
- 4.3 Build Specifications
- 4.4 Attack Flow for Azure DevOps

Module 4: Attacking Azure DevOps

4.5 Demo 01: Environment Variables Exfiltration

4.6 Demo 02: Pipeline Identity Token Exfiltration

4.7 Demo 03: Enumeration with PAT

4.8 Demo 04: Production App Token via SSRF

4.9 Takeaways

CWL
CyberWarFare Labs

THANK YOU