Offensive Operations in Kubernetes and GKE (Bootcamp)

Module 1 : Attacking Docker Environments

- 1.1 Docker Attack Surface Reconnaissance
  - 1.1.1 Discovery of Exposed Docker APIs and Sockets
  - 1.1.2 Container Registry Enumeration and Image Discovery
- 1.2 Docker Exploitation Techniques
  - 1.2.1 Abuse of Docker Daemon for Code Execution
  - 1.2.2 Container Escape and Host Breakout Techniques
- 1.3 Real-World Attack Scenarios and Case Studies
  - 1.3.1 Exploitation of Misconfigured Docker APIs in Production
  - 1.3.2 Container Supply Chain and Malicious Image Attacks

Module 2 : Attacking Kubernetes Clusters

- 2.1 Kubernetes Threat Modeling & Attack Surface Mapping
- 2.2 External Attack Surface Exploitation
  - 2.2.1 Unauthenticated Attack Vectors
    - 2.2.1.1 Cluster Fingerprinting and Environment Profiling
    - 2.2.1.2 Identification & Exploitation of Misconfigured Components
  - 2.2.2 Authenticated Attack Vectors
    - 2.2.2.1 Initial Access via Credential Abuse
      - A. Abuse of Leaked Credentials
      - B. Cloud Credential and Identity Abuse
    - 2.2.2.2 Post-Access Enumeration
      - A. RBAC and Permission Mapping
      - B. Cluster Resource Discovery
    - 2.2.2.3 Initial Access from Compromised Workloads
      - A. Exploitation of Vulnerable Application Containers

Module 2 : Attacking Kubernetes Clusters

- 2.3 Internal Cluster Attacks (Post-Compromise Tradecraft)
  - 2.3.1 Privilege Escalation Techniques
    - 2.3.1.1 RBAC Misconfiguration Abuse
    - 2.3.1.2 Exploitation of Privileged Pods
  - 2.3.2 Persistence Mechanisms
    - 2.3.2.1 Backdoored Deployments and Workloads
    - 2.3.2.2 Malicious CronJobs for Scheduled Access
  - 2.3.3 Defense Evasion Techniques
    - 2.3.3.1 Log and Event Manipulation
    - 2.3.3.2 Resource Name Masquerading
  - 2.3.4 Data Exfiltration
    - 2.3.4.1 Extraction of Secrets and Sensitive Data
    - 2.3.4.2 Abuse of Kubernetes API for Data Access
  - 2.3.5 Lateral Movement
    - 2.3.5.1 Pod-to-Pod Pivoting Across the Cluster
    - 2.3.5.2 Internal Network and Service Abuse
    - 2.3.5.3 Pivoting to External Cloud Resources

Module 3 : Attacking GKE Clusters

3.1 GCP Fundamentals for Red Teamers

3.2 GKE Architecture and Trust Boundaries

3.3 Initial Access and Enumeration

3.4 Privilege Escalation via IAM and Workload Identity

3.5 Persistence Mechanisms in GKE

3.6 Defense Evasion Techniques

3.7 Data Exfiltration

3.8 Lateral Movement Across Kubernetes and GCP

CWL
CyberWarFare Labs

THANK YOU