Day 57

Exploitation Analyst

Introduction to Keycloak and Basic Configuration:

What is Keycloak?

Keycloak is an open-source Identity and Access Management (IAM) tool developed by Red Hat. It provides features such as single sign-on (SSO), user authentication and authorization, role-based access control (RBAC), and federated identity (integration with external identity providers like Google, LDAP, or Active Directory).

With Keycloak, applications don't need to handle login, password storage, or session management themselves—these are centralized and secured by Keycloak. It supports modern protocols like OAuth2.0, OpenID Connect, and SAML, making it widely used for securing web apps, mobile apps, and APIs.

Some main features:

- Single Sign-On (SSO): Log in once to access multiple applications.
- Identity Brokering & Social Login: Integrates with external providers (Google, Facebook, GitHub, LDAP, Active Directory).
- User Federation: Sync users from existing databases or directory services.
- Authorization Services: Supports role-based and fine-grained access control (RBAC & ABAC).
- Standard Protocols: Supports OAuth 2.0, OpenID Connect, and SAML 2.0.
- User Management: Provides self-service account management (profile updates, password resets, MFA setup).
- Multi-Factor Authentication (MFA): Adds extra layers of security.
- Admin Console: Centralized UI for managing users, roles, sessions, and settings.
- Extensible & Customizable: Themes, custom providers, and integration with apps.
- Session Management: Centralized logout and session handling across apps.

Key concepts of Keycloak:

- Realm – A space in Keycloak where you manage users, roles, and applications. (e.g., one realm for dev, one for prod).
- Client – An application or service that uses Keycloak for login/authentication (web app, API, mobile app).
- User – An individual identity stored in Keycloak, with credentials, roles, and permissions.
- Role – A label that defines permissions (e.g., *admin*, *editor*, *viewer*), assigned to users or groups.
- Group – A collection of users that can share roles/permissions.
- Identity Provider (IdP) – External authentication sources integrated with Keycloak (Google, LDAP, AD, etc.).
- Authentication Flow – The process Keycloak uses to verify a user (can include MFA, password, OTP, etc.).
- Authorization Services – Define and enforce fine-grained access control to resources.

- Tokens – Security artifacts (like JWTs) issued by Keycloak for authentication/authorization (Access Token, Refresh Token, ID Token).
- Federation – Connecting to external user stores so Keycloak can manage them.

--The End--