**Day 29**





**“CLOUD SECURITY”**

**AWS Application Security Features**:

* **AWS IAM** – Manages identities, authentication, and fine-grained access control.
* **AWS WAF** – Protects web apps from common exploits (SQLi, XSS) via traffic filtering rules.
* **AWS Shield** – Provides DDoS protection (standard + advanced).
* **Amazon CloudFront** – Secure CDN that delivers content with low latency.
* **AWS Firewall Manager** – Centralized firewall rule management.
* **Amazon Inspector** – Automated vulnerability assessment for apps on AWS.
* **Amazon CloudWatch** – Monitors applications, performance, and security logs.

**AWS Identity and Access Management (IAM)**

* **Purpose**: Securely controls *who* can access AWS services/resources and *what* actions they can perform.
* **Features**:
  + Shared access via users/groups (no need to share root credentials).
  + Granular permissions per resource/service.
  + Secure app access for EC2 workloads.
  + MFA for stronger authentication.
  + Identity federation (single sign-on between cloud & on-prem).
  + Logging with CloudTrail.

**Application Security in Cloud**

* **Compliance**: Supports PCI DSS for credit card data security.
* **Centralized Access Control**: IAM integrated across AWS services.
* **Password Management**: Rotation, reset, and policy enforcement.
* **Policies & Groups**: Organize users in groups, apply least privilege via policies.