Day 56

Exploitation Analyst

Basic of IAM: IAM concepts and Techniques:

What does IAAA means in Security?

Identification, Authentication, Authorization, and Accountability. Here's a quick breakdown:

1. Identification – Claiming an identity (e.g., entering a username, user ID, or email).
2. Authentication – Proving that the identity is valid (e.g., password, OTP, biometrics, certificate).
3. Authorization – Granting or restricting access to resources based on permissions/roles (e.g., read/write access).
4. Accountability – Tracking and logging user actions to ensure responsibility and traceability (e.g., audit logs).

What is IAM?

Identity and Access Management (IAM) is a framework of policies, processes, and technologies that ensures the right individuals or systems have the appropriate access to resources at the right time. It manages digital identities, authenticates users, controls their permissions, and monitors their activities to protect sensitive data and systems. By enforcing principles like least privilege, role-based access, and strong authentication, IAM reduces security risks, prevents unauthorized access, and helps organizations maintain compliance.

Brief breakdown of IAM (Identity and Access Management) fundamentals:

1. Identity – Establishing *who* a user, device, or service is. (e.g., employee ID, username, service account)
2. Authentication – Verifying that identity using credentials (passwords, biometrics, MFA, certificates).
3. Authorization – Defining what the identity can access or do (roles, policies, permissions).
4. Accountability – Logging and monitoring activities to ensure compliance and traceability.

Importance of IAM:

- Prevents unauthorized access & data breaches.
- Enforces least privilege & role-based access.
- Automates user lifecycle (joiners, movers, leavers).
- Ensures compliance with security regulations.
- Improves user experience via SSO & MFA.

Rights and Privileges in IAM:

In IAM, *rights and privileges* define what a user, device, or service can do after being authenticated:

- Rights – Permissions to access specific resources (e.g., right to log in, read a file, use an app).
- Privileges – The level of control or actions allowed (e.g., admin privilege to create users, delete data, change settings).

Account administration and Domain Security:

Account Administration

- Involves creating, managing, and deleting user accounts.
- Covers password policies, MFA setup, access reviews, and role assignments.
- Ensures accounts follow the principle of least privilege and are updated when users change roles or leave.

Domain Security

- Protects all accounts, devices, and resources within a domain (e.g., an Active Directory environment).
- Includes centralized authentication, group policies, domain controllers, and trust management.
- Enforces consistent security policies (password rules, account lockouts, access restrictions) across the network.

--The End--