Below is a **sentence-by-sentence breakdown** of the document titled **"Privileged Access Management Notes"**, rewritten as **highly detailed study notes** tailored for **CompTIA A+ 220-1102 Objective 2.1 (Security Concepts)**. This version avoids decimal-style numbering, uses clean formatting, and is designed for **easy copy-pasting into Microsoft Word** with minimal spacing.

**Privileged Access Management (PAM) – Study Notes**

**CompTIA A+ 220-1102 | Objective 2.1 – Security Concepts**

**1. What is Privileged Access Management (PAM)?**

* PAM is a **security solution** that helps organizations **restrict and control privileged access** within IT environments.
* It is a **critical part** of an organization’s security strategy because it:
  + Prevents data breaches.
  + Enforces **least privilege access**, meaning users receive only the minimum necessary permissions to perform their tasks.

**2. Purpose and Risk Mitigation**

* PAM uses **policies, procedures, and technical controls** to:
  + Prevent **malicious abuse** of privileged accounts.
  + Reduce risks from **poorly configured access permissions**.
* Privileged accounts often have administrative or root access, making them **prime targets** for attackers if not properly secured.

**3. Core Components of PAM**

PAM consists of **three key components**:

**a. Just-in-Time (JIT) Permissions**

* Grants **administrative access only when needed** and for a **limited period**.
* Helps minimize the **window of exposure** for unauthorized access or privilege misuse.
* **Example:** A system administrator is granted access to a server only during a scheduled maintenance task. As soon as the task is completed, access is automatically revoked.
* This model ensures that no one retains continuous privileged access to critical systems.

**b. Password Vaulting**

* Involves storing and managing privileged credentials in a **secure digital vault**.
* Access to the vault usually requires **multi-factor authentication**.
* Ensures that:
  + Passwords are **centrally managed**.
  + There’s a **record of who accessed what credentials and when**.
* **Example:** Dion Training stores Windows admin and Linux root credentials in a shared vault, requiring secure login to retrieve and use them.

**c. Temporal Accounts (Temporary Accounts)**

* Created to provide **time-limited access** to specific resources or systems.
* Automatically **disabled or deleted** after a set time period or task completion.
* **Example:** A contractor is granted temporary access to a corporate network during a software deployment project. Once the project ends, access is removed automatically.
* Ensures that **no lingering access remains** once the account is no longer needed.

**4. Summary of PAM Principles**

* PAM is based on **control and accountability** for access to sensitive systems.
* Its three components work together to:
  + Limit access exposure (JIT),
  + Secure credential storage (Vaulting),
  + Eliminate unnecessary accounts (Temporal Accounts).
* These methods reduce the chances of **internal and external misuse** of privileged credentials.