Privileged Access Management
About Me:

- I, Sudheer Karanam, have over 19+ years of experience in IT Industry with over 12+ years dedicated to InfoSec.

- My expertise includes many of Information security domains such as:
  
  • User Profile Management,
  • PII (Personally identifiable information),
  • Single Sign On,
  • OAuth, OpenId,
  • Device Identity,
  • Risk Adaptable Access controls,
  • Privileged Identity and Access Management,
  • Secrets Management,
  • PCI (Payment Card Industry) standards & processes.

- I hold Security industry’s leading certifications such as Certified Ethical Hacker (CEH), CISSP.
Agenda:
- Privileged Access Management
  - What?
  - Why?
  - Key Benefits
- What does PAM do?
- PAM Solution types:
- PAM Implementation:
- Key players:
- Q & A
What is Privileged Access Management (PAM)?

- **What are privilege actions?**
  - Ex:
    - Modify System config.
    - CRUD operations on User/System accounts.
    - Administrative activities.

- **What are privileged accounts?**
  - Any accounts (human/system) with special/extra rights (which go beyond that of an ordinary user) to operate on applications, infrastructure, or data. Ex: Root users, Admin accounts, System accounts, Emergency accounts, Service accounts etc.

- **What is PAM?**
  - Is set of strategies/policies to safeguard administrative credentials and detect/alert/prevent malicious activities such as steal, destroy data or files on IT infrastructure.
Why PAM?

- Threats:
  - Employees (Weakest link in cyber security).
  - External Malicious actors.

- According to the Verizon Data Breach Investigation 2021 report, 61% of surveyed data leaks involved privileged credentials. And the cost of this type of attack is also higher.

- According to IBM in the Cost of Data Breach Report 2021, while the average cost of a data leak is usually $4.24 million, when the data leak involves privileged credentials, this value can reach $4.37 million.
Key Benefits of PAM:

- **Malware protection:** Malwares usually require and operate in high privilege layers of system, with PAM its movement can be prevented or have its speed reduced.

- **Compliance** with important security (ex: SOX, HIPPA, NIST etc) & data protection (GDPR, CCPA etc) standards,

- **Improved Operational Efficiency:** With principle of least privilege only relevant permissions are assigned and maintained.
What does PAM do?

- **Centrally manage access** and can be a great help in preventing insecure password stores and shares.

- Implement **principle of Least Privilege** ensuring only minimal required access permissions to users.

- Can track **authorized/unauthorized** activities performed by privileged users **in real time**, monitor and ensure compliance to security standards.

- Maximize **security** with reduced **complexity** and increased **visibility**.

- Note: Gartner suggests it is impossible to manage risk without specialized PAM tools.
PAM Solutions:

- Privileged Account and Session Management (PASM):
  - Credentials are securely created and distributed through PAM, similar to a password manager. Thus every time a user needs access they get an account with privileges, with all its activities recorded.
  - PASM offers:
    - Real-time monitoring.
    - Access control for shared accounts with MFA.
    - Remote session
    - Session Recording.

- Secrets Management:
  - Secrets: SSH keys, passwords, OAuth tokens, API keys.
  - Dynamic vs Static accounts.

- Privileged Elevation and Delegation management (PEDM):
  - Provide privileges based on role of the user.
  - JIT/ZSP Access.
Advanced PAM:

- Zero standing privileges (ZSP).

- Use ephemeral identities and credentials (No password vaults or password rotation)

- Privileged Task Automation.

- Advance analytics.
**PAM implementation:**

- The implementation of PAM involves three aspects: tools, people, and processes. Along with state of the art tool, it is very pertinent to invest in process optimization and training people.

  **Pre-requisites:**
  - Inventory of accounts, credentials, systems.
  - Inventory of H2M Operations.
  - Inventory of M2M Operations.

  **Implementation:**
  - Enable real time session-activity tracking for detecting any deviants/abuses.
  - Enable session recordings.
  - Integrate with Secret management tool.
  - Extremely critical infrastructure : Ensure high-availability and recovery mechanisms.

  **Advanced :**
  - Robotic process automation (RPA).
  - Cloud infrastructure entitlement management (CIEM).
Key players:
Q & A
Appendix:

References:
- https://www.ssh.com/academy/iam/pam
- https://senhasegura.com/privileged-access-management-pam-a-complete-guide/
- Guidance for Privileged Access Management — Gartner