Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Enterprise Security Management - Privileged Access Management

Maintained by: NIAP

Unique Identifier: tbd

Version: 0.4

Status: draft

Date of issue: 05 October 2022

Approved by:

Supersedes:

Background and Purpose

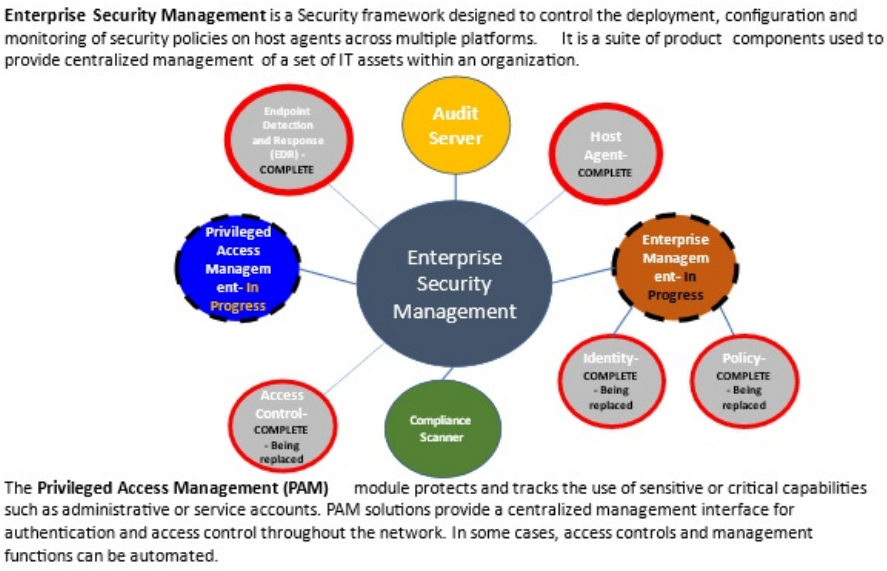

Figure esm-framework: ESM Framework

Certain capabilities on an Enterprise network require an enhanced level of protection. For instance:

- Access to mission critical or sensitive data
- The ability to manage or bypass network security controls
- The ability to control machines or applications (e.g. Industrial Control Systems).

These capabilities are usually restricted to privileged accounts and are protected by restricting access to those accounts.

A Privileged Access Management solution manages these privileged accounts and associated credentials in order to provide increased granularity of control, improved monitoring of privileged activity, and to reduce the attack surface of the privileged accounts.

PAM solutions (as defined by Gartner) typically offer one or more of these features:

- Discover, manage and govern privileged accounts (i.e., accounts with superuser/administrator privileges) on multiple systems and applications.
- Control access to privileged accounts, including shared and emergency access.
- Randomize, manage and vault credentials (password, keys, etc.) for administrative, service and application accounts.
- Provide single sign-on (SSO) for privileged access to prevent credentials from being revealed.
- Control, filter and orchestrate privileged commands, actions and tasks.
- Manage and broker credentials to applications, services and devices to avoid exposure.

- Monitor, record, audit and analyze privileged access, sessions and actions.

Use Cases

As a stand-alone physical appliance.

As the only guest on a virtual platform.

As one of several guests on a virtual host platform.

Notes on using a shared virtual host

Not Recommended. This use case may be covered in a future iteration of this profile.

Host Platform administrators have full access to guest systems – in this case the PAM. This is not an issue if the sole responsibility of the virtual platform administrators is to manage the PAM itself.

A virtual PAM is exposed to potential attacks from peer tenants on the host system. Peer tenants would have to be fully trusted. The following services, if provided by separate applications, may run on the same platform without being within the TOE. These services are trusted and should be certified if possible.

- Directory and Enrollment services
- Audit services
- Authentication services

VM isolation mechanisms are not assumed to be sufficient to protect against managed credential leakage to other tenants.

Categories (as defined by Gartner):

Privileged account and session management (PASM). The PAM protects accounts by vaulting the credentials. Users (human or automated) first connect to the PAM, which then establishes and monitors the session. [Diagram: User ->PAM->managed account]

Privilege elevation and delegation management (PEDM). Host-based agents enable the users to execute specific privileged commands. Again, sessions are typically monitored. (Host based agent requirements could be covered by the ESM Host Agent module.) [Diagram: User->host agent contained within host]

Credentials management. A credential vault that manages machine-to-machine credentials. [Diagram: M1 to/from credential vault; M1 to M2]

While password management solutions for individual users may fit the definition of PAM, they are outside the scope of this profile.

Resources to be protected

The primary purpose of a PAM solution is to protect the privileged accounts or privileged access mechanisms that are under management by the PAM. To that end, the following resources and functions need to be protected:

- Audit Information (Both PAM functional audit information and Session Monitoring data)
- Credentials to be managed by the PAM (Credentials to access the controlled assets)
- Credentials to access and administer the PAM
- Access Policies to be managed by the PAM.
- Communications to or from the PAM solution.
- Backup and recovery data, and all other resources required to recover the network in the event of a PAM failure.

Attacker access

(Non-Administrative) users *may* be malicious in nature. Users may attempt privilege escalation either on the assets for which they are permitted access, or other assets managed by the PAM to which they have no permissions.

The following assumptions are made about attackers' ability to develop attacks:

- An attacker has an arbitrary amount of time to analyze the behavior of the product, its interaction with its platform, and the data it transmits over the network.
- An attacker is able to acquire their own copy of the target product and study its behavior on a platform that they control.

The attacker is expected to engage in the following general classes of attack:

- Network eavesdropping, in which an attacker may monitor and gain access to data exchanged between the product and other endpoints.
- Network attack, in which an attacker may initiate malicious communications with the product or alter communications between the product and other endpoints.
- Local attack, in which an attacker has gained the ability to execute code or instructions on the PAM platform, which may be used to escalate privilege or access data without authorization.
- Limited physical access attack, in which an attacker may attempt to access data on the system by virtue of being physically present for a limited period of time. This limited physical access does not include attacks in which the attacker could disassemble the system to gain access to its storage media or manipulate the product's underlying hardware and firmware. Systems used for working remotely, such as laptops and tablets, for which an attacker could gain longer physical access to, should apply additional protections that are provided by products evaluated against other Protection Profiles (e.g. FDE cPP).

Attack Scenarios

Privilege Escalation could entail:

1. An unprivileged network user gains network privileged accesses.
2. A user with some privileged accesses gains additional unauthorized privileged accesses.
3. Any unauthorized user gaining the ability to administer or control the PAM itself.

Passive Eavesdropping Attacks

- Recovering credentials through network traffic.

Active Network Attacks

- Privilege escalation via credential replay attack.
- Privilege escalation via exploitation of the network interface.
- Gain access to protected devices or accounts by bypassing the PAM.
- Denial of service via packet flooding.
- Denial of service via exploitation of the network interface.

Local attacks

- A user on the PAM is able to perform a privilege escalation attack through command execution.
- A user on the PAM is able to load / execute codes or scripts that enable privilege escalation.
- A user on the PAM is able to access or manipulate protected data.

Limited Physical Access

- Power cycling, turning off, or rebooting the host system
- USB-memory device enabled attacks: software load or replacement, data extraction.
- Other cabling attacks – attaching unauthorized devices, making unauthorized connections.

Essential Security Requirements

- Internal protection of credentials
  - Key material for encrypting data-at-rest and data-in-transit must be secured in a way that can’t be accessed by unauthorized users or processes.
  - There needs to be a method of updating keys and destroying old keys in a secure fashion. There may be system recovery considerations here.
- Managed credential generation requirements
  - Be able to create and manage credentials of various privileges.
  - Hit minimum standards for managed credentials with ways to increase the security through additional controls if need be.
  - Have a set policy in place for creating, modifying, or removing privileged accounts.
  - Apply appropriate RNG or other credential generation requirements. Reference NIST SP 800-63b.
  - Support use of multi-factor authentication.
- Managed credential storage requirements
  - Keep the credentials encrypted and limit those who would be able to access the plaintext data.
  - Do not access the data in plaintext, but check against cryptographic hashes
- Managed access control policy requirements
  - Limit and protect the ability to manage PAM user permissions.
- Communication channel protection.

    - All communications going to or from the PAM needs to be encrypted with adequate cryptography, e.g. TLS, DTLS, or SSH. There can be no option for anything to be transmitted in plaintext.
    - Certificate management requirements.
- Replay attack protection
    - Possible mechanisms:
        - Timestamps can be included in the transmissions to make sure that any hashes used to login can’t be repeated.
        - Unique cryptographic session IDs for each transmission.
        - One time passwords for each session, like in RSA’s securID.
    - Encrypting messages preventing tokens or hashes from being sniffed
- Session monitoring requirements
    - Optional Real time monitoring alert capability
    - General audit requirements – write only, sensible storage management requirements, etc.
- Recovery and Ransomware concerns and requirements
    - Must be able to recover PAM generated credentials in the event of loss of the PAM
    - Have the ability to create a cryptographically secure backup file that can be stored in a safe location
    - Ability to backup and restore the data in a secure way. Require strong credentials to access.
- Requirements for Directory or (authentication) server interactions.
    - Establish secure communications between the service(s) and the PAM
    - Define and protect the accounts that would be used by the PAM and the service.
- PAM administration security mechanisms.
    - Ability to customize based on customer need – This may be a capability that requires protection.
    - Have a policy for how to access / manage the PAM securely.
        - Control interface should be separated from the user channels.
        - User facing interface must be separated from the protected resource interface
    - Use of network segmentation to control connection with the PAM
    - Recommend MFA for accessing the PAM. (Reference NIST SP 800-63b)
- Physical protection
    - Provide means of detecting, alerting or preventing the unauthorized use of portable media to load software or remove data.
- Auditing requirements
    - Provide a means to record and track the use of sensitive functions.

Assumptions

The following assumptions are made for the TOE and its operational environment:

- PAM Administrators are not malicious, and operate the system in compliance with approved enterprise security policy.
- The application relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the application.

Optional Extensions

N/A

Outside the TOE's Scope

The following list contains items that are explicitly out-of-scope for any evaluation against the module:

- External authentication services. (Similar to external directory services.)
- Enterprise level audit management services. (I.E. once the information is passed from the PAM to external audit or orchestration solutions, it is outside the scope.)
- Network routing, switching, and segmentation.