USE CASE I Financial Services

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PRIVILEGED ACCOUNT MANAGEMENT

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of privileged account management (PAM) through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the issues surrounding PAM including background and challenges, goals, and potential benefits. If you would like to propose another architecture or know of products that might be applicable to this challenge, please contact us at financial_nccoe@nist.gov.

BACKGROUND

Privileged accounts provide elevated, often unrestricted access to an organization's underlying information systems and technology, making them rich targets for both external and internal malicious actors. Often referred to as "the keys to the kingdom," these accounts have been used in successful attacks to gain access to corporate resources and critical systems (e.g. "crown jewels"), resulting in data breaches.

As a result of this elevated access and capability, privileged accounts must be carefully controlled and monitored. PAM is a domain within identity and access management that focuses on monitoring and controlling administrative accounts/users within an organization. Many organizations use PAM systems to provide oversight of these powerful accounts. By implementing a PAM system, organizations are able to protect, monitor, and audit privileged account access, which in turn can reduce the possibility of data destruction, data exfiltration, and system failure.

CHALLENGE

Developing a comprehensive PAM capability that controls a user's access without hindering their ability to perform certain job tasks, presents several challenges, including, but not limited to:

- regulatory compliance (managing, monitoring, and auditing activity)
- internal malicious activities
- abuse of rights
- employee mistakes
- securing administrative access to cloud infrastructure
- malware account escalation and account takeover
- third-party access management

GOAL

The goal of this project is to demonstrate a PAM capability that effectively protects, monitors, and manages privileged account access including life-cycle management, authentication, authorization, auditing, and access controls.

BENEFITS

Implementing a comprehensive PAM capability can benefit organizations by:

- managing privileged account credentials and access rights to control users' access to IT systems and infrastructure without compromising their ability to perform approved job functions
- monitoring privileged account activity to identify unauthorized access
- auditing and reporting suspicious activity to enable a quick response to threats

Ultimately this project will reduce the ability of external and internal malicious actors to exploit privileged accounts to gain entry to an organization's technology infrastructure, e.g., networking systems, applications, and operating systems.

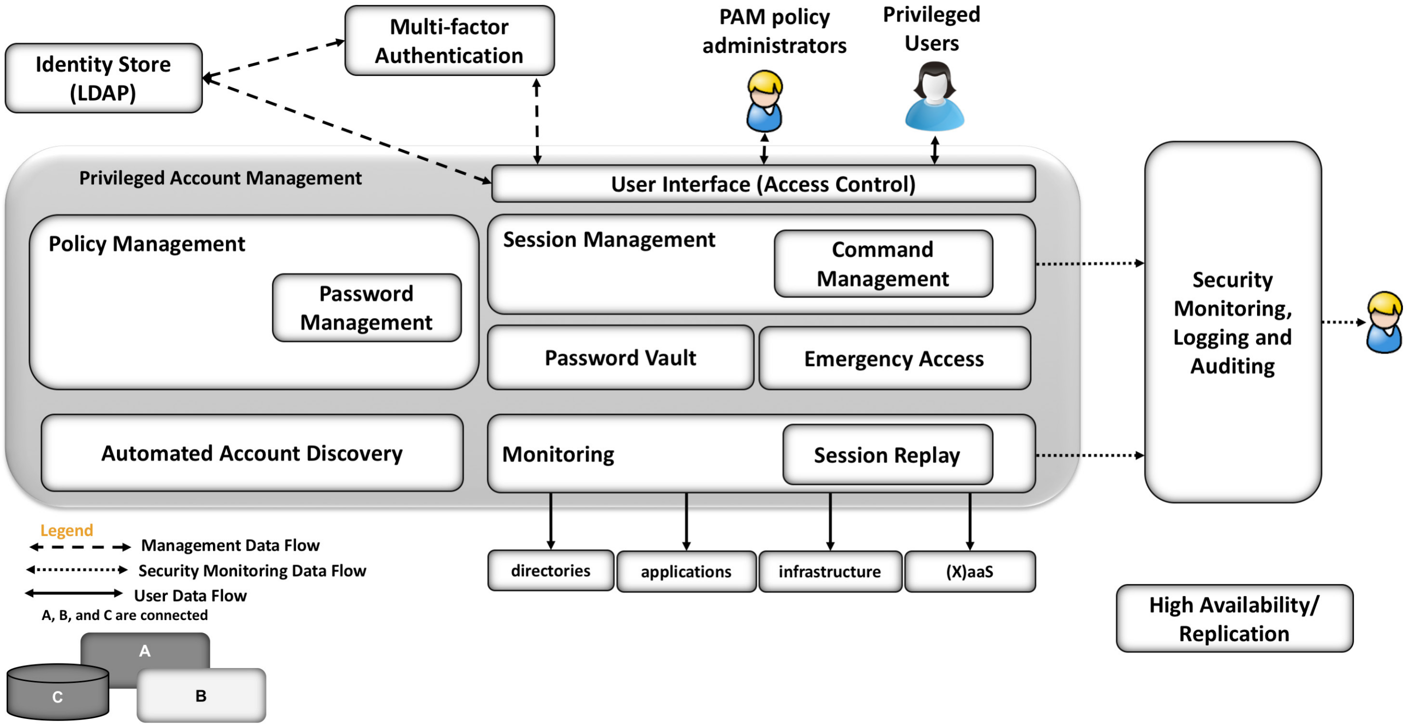
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

This high-level architecture diagram introduces privileged account management into the information technology infrastructure of an organization between the IT elements and the privileged users (administrators).


Identity Store (LDAP)
Multi-factor Authentication
PAM policy administrators
Privileged Users
Privileged Account Management
User Interface (Access Control)
Policy Management
Password Management
Session Management
Command Management
Password Vault
Emergency Access
Automated Account Discovery
Monitoring
Session Replay
Security Monitoring, Logging and Auditing
directories
applications
infrastructure
(X)aaS
High Availability/ Replication
Legend
Management Data Flow
Security Monitoring Data Flow
User Data Flow
A, B, and C are connected
A
B
C

COMPONENT LIST

This solution includes, but is not limited to, the following components:

- privileged account control
- privileged account command filtering (allow or deny specific commands, such as disk formatting)
- multifactor authentication capability
- access logging/database system
- password management
- separation of duties management
- support least privileged policies
- password obfuscation (hiding passwords from PAM users)
- temporary accounts
- log management (analytics, storage, alerting)

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit: https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email financial_nccoe@nist.gov.

April 2018