Center for Development of Security Excellence

CDSE

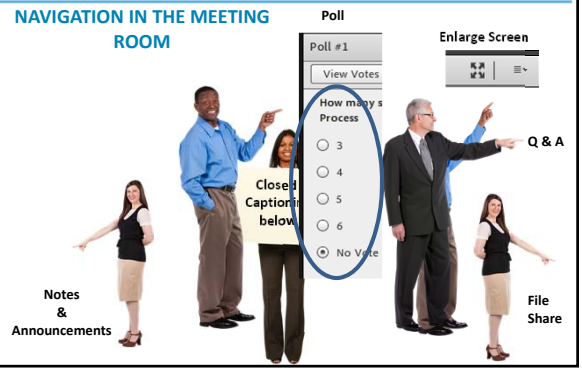
Learn. Perform. Protect.

Best Practices and Vulnerabilities for Privileged Accounts

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

NAVIGATION IN THE MEETING ROOM



Best Practices and Vulnerabilities for Privileged Accounts

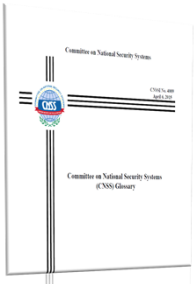
CDSE

Overview

- Define Privilege Account
- Identify Common Types of Privileged Accounts
- Identify Risks Associated with Privileged Accounts
- Discuss Some Best Practices

Privileged User and Privileged Account

- **Privileged User**
  A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
- **Privileged Account**
  An information system account with approved authorizations of a privileged user.



4

Best Practices and Vulnerabilities for Privileged Accounts
CDSE

Responsibilities

Privileged Users (e.g., System Administrators) must:

- Configure and operate IT within the authorities vested in them according to DoD cybersecurity policies and procedures.
- Notify the responsible ISSO or, in the absence of an ISSO, the responsible ISSM, of any changes that might affect security posture.

IAW DoD 8500.01, March 14, 2014

5

Best Practices and Vulnerabilities for Privileged Accounts
CDSE

Workforce Categories and Specialties

Category

- IA Workforce Technical
  - IAT I
  - IAT II
  - IAT III
- IA Workforce Management
  - IAM I
  - IAM II
  - IAM III

Specialty

- Computer Network Defense Service Providers (CND-SPs)
- IA System Architects and Engineers (IASAEs)

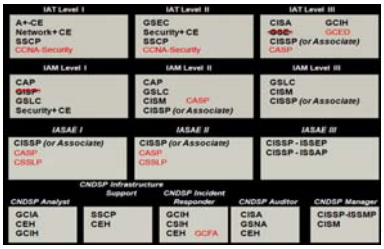
6

Privileged Users

QUALIFICATIONS

Personnel filling positions with privileged access must satisfy both preparatory and sustaining DOD IA training and certification requirements

Table AP3.T2
DoD Approved
Baseline Certifications



Best Practices and Vulnerabilities for Privileged Accounts

Polling Question 1:

Do you believe that privilege users pose a threat in your organization?

- ❑ Yes
- ❑ No

8

Best Practices and Vulnerabilities for Privileged Accounts

Cyber Attacks

Database admin steals 2.3M consumer records at Fidelity National subsidiary

Medco sys admin gets 30 months for planting logic bomb

Inside saboteur could have crippled pharmacists' ability to check for deadly drug interactions, U.S. attorney says

Edward Snowden Lea
"Thousands" of NSA
uments

San Francisco IT worker arrested in hijacking of city network

Disgruntled city worker in jail on $5 million bail after allegedly locking administrators out of the city's wireless area network.

9

U.S.

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

Common Privileged Accounts

System Administrator Account
Database Administrator Account
Web Administrator Account
Network Administrator Account
Application Developer Account
System Accounts
Service Accounts

Service Accounts

Consider using

- LocalService
- NetworkService

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

Poll Question 2:

At a minimum, how often should privileged accounts passwords be changed?

- ❑ 30 days
- ❑ 60 days
- ❑ 90 days

13

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

PASSWORDS

Sorry, but your password must contain at least an uppercase letter, a lowercase letter, a number, and a special character.

14

Best Practices and Vulnerabilities for Privileged Accounts

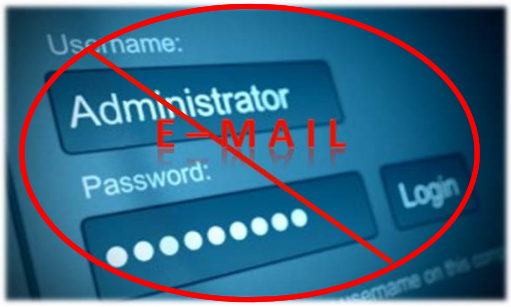
CDSE

Privileged Users Should

NEVER

Use Privilege Accounts to Perform Day to Day Functions

Best Practices and Vulnerabilities for Privileged Accounts



Best Practices and Vulnerabilities for Privileged Accounts

Least Privileges

Grant individuals access to only those specific resources and functions required to carry out their current responsibilities

Best Practices and Vulnerabilities for Privileged Accounts

Separation of Duties

Divide roles and responsibilities among multiple people to exclude the ability of one person to perform all privilege actions on a system

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

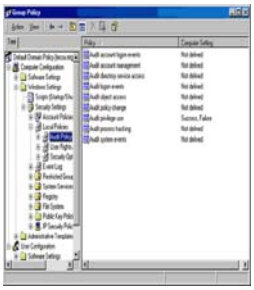
Audit Privileged Use

Auditing Successes

- Generates an audit entry when the exercise of a privileged user right succeeds

Auditing Failures

- Generates an audit entry when the exercise of a privileged user right fails



Best Practices and Vulnerabilities for Privileged Accounts

CDSE

Audit "Sensitive Privilege Use"

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

Policy

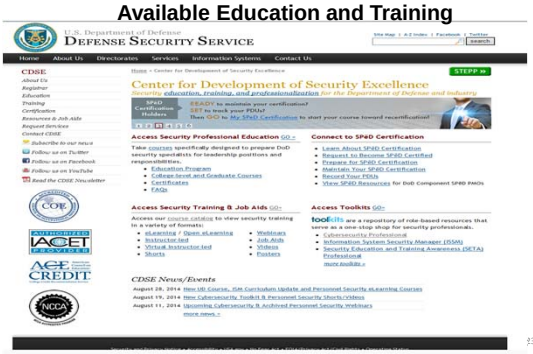
Develop a policy that defines how privileged accounts will be managed.

Best Practices and Vulnerabilities for Privileged Accounts

Conclusion

Best Practices and Vulnerabilities for Privileged Accounts

Available Education and Training



Best Practices and Vulnerabilities for Privileged Accounts

Questions

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

Feedback

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you're able to share these in the questionnaire.

25

Best Practices and Vulnerabilities for Privileged Accounts

CDSE

Cybersecurity Training Products and POC

Past Webinars

- Information Security Continuous Monitoring
- Monthly Cyber Awareness
- Trusted Downloading
- NISP C&A Process and OBMS

All Other Training

- CDSE Cybersecurity

Renee Hartsfield
Work: (410) 689-1373

E-mail:
dorothy.hartsfield@dss.mil
cybersecurity.training@dss.mil

26