Best Practices and Vulnerabilities for Privileged Accounts

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.

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

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

<table>
<thead>
<tr>
<th>Baseline Certifications</th>
<th>Best Practices and Vulnerabilities for Privileged Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Polling Question 1: Do you believe that privilege users pose a threat in your organization?</td>
</tr>
<tr>
<td></td>
<td>- Yes</td>
</tr>
<tr>
<td></td>
<td>- No</td>
</tr>
</tbody>
</table>

Cyber Attacks

Edward Snowden Leaks "Thousands" of NSA Documents

San Francisco IT worker arrested in hijacking of city network

Polling Question 2: Do you believe that privilege users pose a threat in your organization? 
- Yes
- No

Polling Question 3: Do you believe that privilege users pose a threat in your organization? 
- Yes
- No
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
Poll Question 2:
At a minimum, how often should privileged accounts passwords be changed?
- 30 days
- 60 days
- 90 days

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

Privileged Users Should
NEVER
Use Privilege Accounts to Perform Day to Day Functions
**Least Privileges**
Grant individuals access to only those specific resources and functions required to carry out their current responsibilities.

**ACCESS DENIED:**
The Principle of Least Privilege

**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.
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

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

Policy

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

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
Email: dorothy.hartsfield@dss.mil
cybersecurity.training@dss.mil