AIX Auditing

Overview

The AIX Auditing subsystem provides comprehensive recording of security-related AIX events that can be used to alert you about potential or actual violations to the system security policy. AIX Auditing tracks user activities critical to preventing, detecting, or minimizing the impact of a security breach. The implementation of auditing allows thorough tracking, alerting, and analysis when something goes wrong. Additionally, determining the cause of a compromise is difficult or impossible without the critical forensic information that AIX Auditing provides.

Technical Details

- AIX Auditing configuration can be streamlined with the use of AIX Enhanced Role Based Access Control
- Many configuration options are available for saving on disk and CPU usage

Common Use Cases

- An AIX organization that would like to learn how to properly configure AIX Auditing
- An AIX organization that would like to mitigate the security risk of a security incident by properly configuring the monitoring of AIX
- An AIX organization that would like to evaluate AIX Auditing in a proof-of-concept environment
- An AIX Organization that would like to fulfill security requirements for implementing detailed logging of security events on AIX

Engagement Process

- Consultant arranges prep call to discuss requirements, scheduling, and agenda
- Consultant works with client to configure AIX auditing in client proof-of-concept environment
- Consultant provides advice on best practice implementation
- Consultant works with client to verify Auditing functions that are most important to the client
- Consultant provides presentations to facilitate knowledge transfer

Deliverables

1. Presentation Slides – an electronic copy of presentation slides
2. Configuration documents – an electronic copy of configuration documents