AIX Security Assessment

Overview

The AIX Security Assessment is designed to provide a comprehensive assessment of your AIX infrastructure. This service assesses over 350 cybersecurity best practices.

The assessment consists of 2 components:

1. Policy Assessment (optional)
2. Host Assessment

Policy Assessment Details

- Based on the subset of CIS v8 safeguards directly related to AIX.
- Over 50 CIS v8 safeguards assessed are security policies that can be implemented to mitigate security risk in AIX infrastructures. For example: Does your organization require multi-factor authentication for all administrative access? Does your organization encrypt sensitive data at rest? Do you disable dormant accounts after a period of 45 days of inactivity?
- Consultant provides a 53-question policy questionnaire to client
- Client completes and returns questionnaire to consultant
- Consultant incorporates results into final report
- **Time requirement**: at least 15 minutes

Policy Assessment Use Cases

- AIX manager wanting to verify the organization is implementing globally accepted security best practices for managing AIX environments
- AIX manager wanting to identify more security tooling to mitigate security risk

Host Assessment Details

- Based on CIS IBM AIX 7.2 Benchmark v1.0.0 – 09-30-2022
- Over 300 CIS AIX Benchmark settings assessed are security hardening settings to be implemented on your AIX instance. For example, verify local AIX configuration uses the SHA-512 password-hashing algorithm for the storing of local passwords
- One or more AIX or VIOS hosts can be assessed
- Any supported level of AIX or VIOS can be assessed
- Data collection script executed on assessment host
- **Time requirement:** 2.5 hours

Host Assessment Use Cases

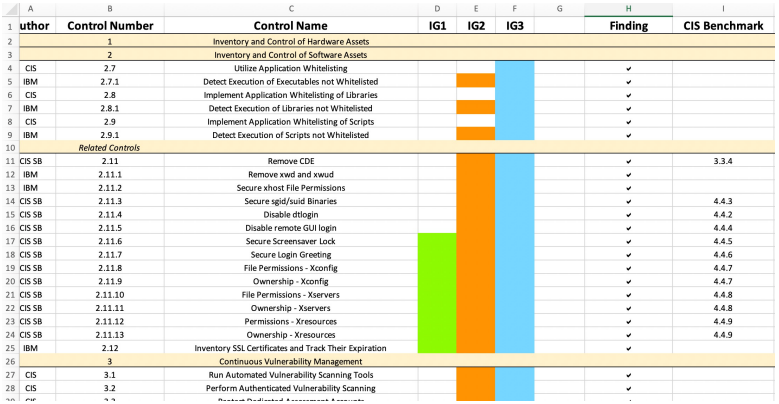
- An AIX Build team that would like to analyze their master NIM image to identify more security hardening settings to add to their NIM build
- An organization that would like to verify a specific AIX instance running critical business applications is secure
- An organization that would like to compare how security settings might differ between virtual machines built in different environments, for example, comparing a PROD host versus a QA or DEV host

Engagement Process

- Consultant arranges prep call to discuss data collection process and to schedule Webex to review assessment results
- Client uploads encrypted tar file and questionnaire to BOX
- Consultant analyzes data and creates deliverables
- Consultant reviews results with client on Webex

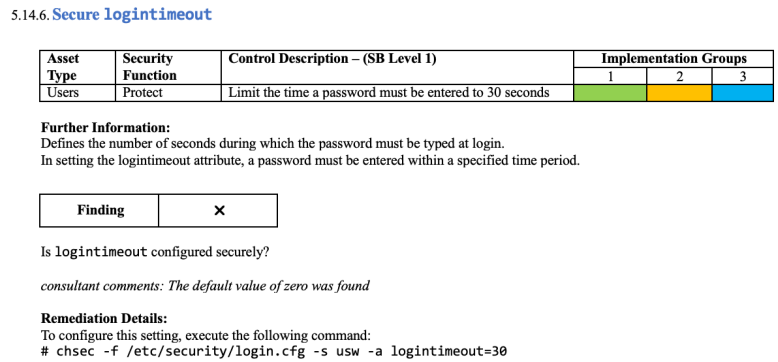
Deliverables

1. AIX Policy Heat Map – this spreadsheet provides a one page view of the results of the Policy Assessment.
2. AIX Security Policy Assessment - this PDF details the results of the Policy Questionnaire completed by the client. Over 50 policy assessment results are detailed in this document. The document provides a hyperlinked Table of Contents to quickly access any of the more than 50 security measures assessed
3. AIX Host Heat Map – (see Fig. 1) the spreadsheet provides a one page view of the results of the host assessment
4. AIX Security Host Assessment – (see Fig. 2) this PDF details the results of the host assessment. Over 300 security assessment results are detailed in this document. The document provides a hyperlinked Table of Contents to quickly access any of the more than 300 security controls assessed
5. Executive Summary – a short summary of the results of the policy and host assessments designed to be presented to executive management



uthor	Control Number	Control Name	IG1	IG2	IG3	Finding	CIS Benchmark
	1	Inventory and Control of Hardware Assets					
	2	Inventory and Control of Software Assets					
CIS	2.7	Utilize Application Whitelisting				✓	
IBM	2.7.1	Detect Execution of Executables not Whitelisted				✓	
CIS	2.8	Implement Application Whitelisting of Libraries				✓	
IBM	2.8.1	Detect Execution of Libraries not Whitelisted				✓	
CIS	2.9	Implement Application Whitelisting of Scripts				✓	
IBM	2.9.1	Detect Execution of Scripts not Whitelisted				✓	
	Related Controls						
CIS SB	2.11	Remove CDE				✓	3.3.4
IBM	2.11.1	Remove xwd and xwud				✓	
IBM	2.11.2	Secure xhost File Permissions				✓	
CIS SB	2.11.3	Secure sgid/suid Binaries				✓	4.4.3
CIS SB	2.11.4	Disable dtlogin				✓	4.4.2
CIS SB	2.11.5	Disable remote GUI login				✓	4.4.4
CIS SB	2.11.6	Secure Screensaver Lock				✓	4.4.5
CIS SB	2.11.7	Secure Login Greeting				✓	4.4.6
CIS SB	2.11.8	File Permissions - Xconfig				✓	4.4.7
CIS SB	2.11.9	Ownership - Xconfig				✓	4.4.7
CIS SB	2.11.10	File Permissions - Xservers				✓	4.4.8
CIS SB	2.11.11	Ownership - Xservers				✓	4.4.8
CIS SB	2.11.12	Permissions - Xresources				✓	4.4.9
CIS SB	2.11.13	Ownership - Xresources				✓	4.4.9
IBM	2.12	Inventory SSL Certificates and Track Their Expiration				✓	
	3	Continuous Vulnerability Management					
CIS	3.1	Run Automated Vulnerability Scanning Tools				✓	
CIS	3.2	Perform Authenticated Vulnerability Scanning				✓	

Fig. 1 - An excel spread sheet will be provided that will indicate the result of each security control being assessed.



5.14.6. Secure logintimeout

Asset Type	Security Function	Control Description – (SB Level 1)	Implementation Groups 1	2	3
Users	Protect	Limit the time a password must be entered to 30 seconds			

Further Information:
Defines the number of seconds during which the password must be typed at login.
In setting the logintimeout attribute, a password must be entered within a specified time period.

Finding	×

Is `logintimeout` configured securely?

consultant comments: The default value of zero was found

Remediation Details:
To configure this setting, execute the following command:

```
# chsec -f /etc/security/login.cfg -s usw -a logintimeout=30
```

Fig. 2 - "Secure Logintimeout" is an example of one of the settings that gets assessed. For each assessed setting, a description, finding and remediation step is provided.