IBM Systems Lab Services

Linux

Linux Security Assessment

Overview

The Linux Security Assessment designed to provide a comprehensive assessment of Linux Security. This service assesses over 300 cybersecurity controls derived from the following:

1. Center for Internet Security 7.1 Controls
2. Center for Internet Security Linux Benchmark settings

These 300 controls are globally accepted security best practices and hardening settings beneficial to any type of business or organization. This service can be provided for RHEL, CentOS, SLES, or Ubuntu running on Power or Intel.

Technical Details

- Over 50 CIS 7.1 controls assessed are globally accepted best practices for securing Linux infrastructures.
  For example, Does your organization require multi-factor authentication for all administrative access?
- Over 250 CIS Linux Benchmark settings assessed are security hardening settings to be implemented on your Linux host.
  For example: Verify the configuration of the SHA-512 password-hashing algorithm on the Linux host

Common Use Cases

- A Linux Build team that would like to analyze their master image to identify more security hardening settings to add to their master image.
- An organization that would like to verify specific Linux virtual machines running critical business applications are secured
- 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
- A Linux manager that would like to verify the organization is in step with globally accepted security best practices for managing Linux environments
- An organization that would like security remediation recommendations provided with guidance on priority and ordering

Service Details

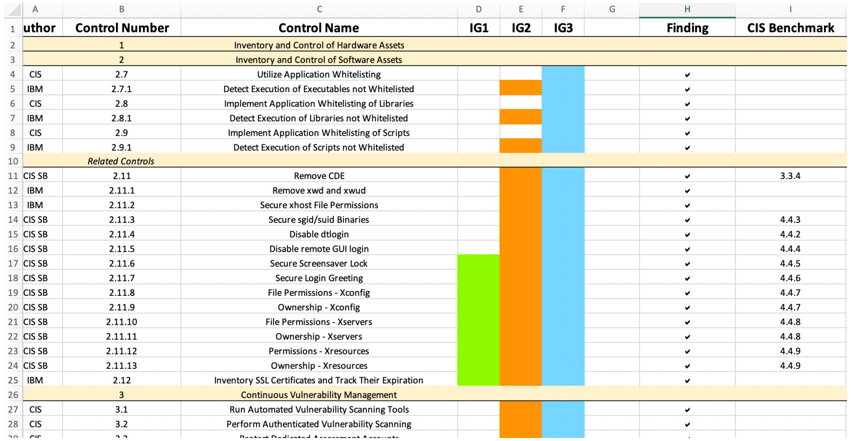
- Data analysis and report generation is done by IBM
- This service requires only a few hours of customer time to run a data collection script and to attend a Webex session to review the results of the assessment
- One or more Linux instances can be assessed, depending on contract terms
- The assessment only reads existing security settings, that is, no settings are altered on the assessment 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 to BOX
- Consultant analyzes data and creates deliverables
- Consultant reviews results with client on Webex

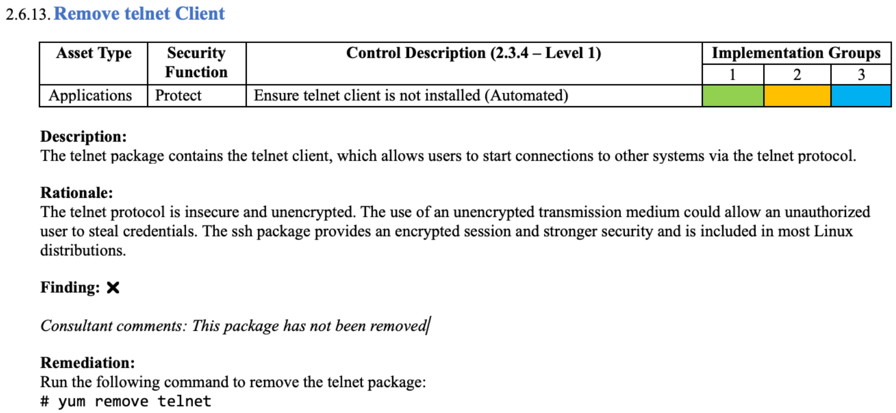
Deliverables

1. Heat Map – (see Fig. 1) the spreadsheet provides a one page view of the results of the assessment
2. Security Assessment Findings – (see Fig. 2) this PDF details the results of the 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
3. Executive Summary – OPTIONAL – a short summary of the results of the assessment designed to be presented to executive management



	A	B	C	D	E	F	G	H	I
1	uthor	Control Number	Control Name	IG1	IG2	IG3		Finding	CIS Benchmark
2		1	Inventory and Control of Hardware Assets						
3		2	Inventory and Control of Software Assets						
4	CIS	2.7	Utilize Application Whitelisting			🟦		✓	
5	IBM	2.7.1	Detect Execution of Executables not Whitelisted		🟧	🟦		✓	
6	CIS	2.8	Implement Application Whitelisting of Libraries			🟦		✓	
7	IBM	2.8.1	Detect Execution of Libraries not Whitelisted		🟧	🟦		✓	
8	CIS	2.9	Implement Application Whitelisting of Scripts			🟦		✓	
9	IBM	2.9.1	Detect Execution of Scripts not Whitelisted		🟧	🟦		✓	
10		*Related Controls*							
11	CIS SB	2.11	Remove CDE		🟧	🟦		✓	3.3.4
12	IBM	2.11.1	Remove xwd and xwud		🟧	🟦		✓	
13	IBM	2.11.2	Secure xhost File Permissions		🟧	🟦		✓	
14	CIS SB	2.11.3	Secure sgid/suid Binaries		🟧	🟦		✓	4.4.3
15	CIS SB	2.11.4	Disable dtlogin		🟧	🟦		✓	4.4.2
16	CIS SB	2.11.5	Disable remote GUI login		🟧	🟦		✓	4.4.4
17	CIS SB	2.11.6	Secure Screensaver Lock	🟩	🟧	🟦		✓	4.4.5
18	CIS SB	2.11.7	Secure Login Greeting	🟩	🟧	🟦		✓	4.4.6
19	CIS SB	2.11.8	File Permissions - Xconfig	🟩	🟧	🟦		✓	4.4.7
20	CIS SB	2.11.9	Ownership - Xconfig	🟩	🟧	🟦		✓	4.4.7
21	CIS SB	2.11.10	File Permissions - Xservers	🟩	🟧	🟦		✓	4.4.8
22	CIS SB	2.11.11	Ownership - Xservers	🟩	🟧	🟦		✓	4.4.8
23	CIS SB	2.11.12	Permissions - Xresources	🟩	🟧	🟦		✓	4.4.9
24	CIS SB	2.11.13	Ownership - Xresources	🟩	🟧	🟦		✓	4.4.9
25	IBM	2.12	Inventory SSL Certificates and Track Their Expiration	🟩	🟧	🟦		✓	
26		3	Continuous Vulnerability Management						
27	CIS	3.1	Run Automated Vulnerability Scanning Tools		🟧	🟦		✓	
28	CIS	3.2	Perform Authenticated Vulnerability Scanning		🟧	🟦		✓	
29	CIS	3.3	Protect Dedicated Assessment Accounts		🟧	🟦		✓	

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



2.6.13. **Remove telnet Client**

Asset Type	Security Function	Control Description (2.3.4 – Level 1)	Implementation Groups		
			1	2	3
Applications	Protect	Ensure telnet client is not installed (Automated)	🟩	🟧	🟦

Description:
The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

Rationale:
The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

Finding: ✗

Consultant comments: This package has not been removed

Remediation:
Run the following command to remove the telnet package:

```
# yum remove telnet
```

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