CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

System Hardening Policy

CSU Bakersfield Policy

Document Number: ITS-90.026
Last Revision Date:
Responsible Office: Information Technology Services
Effective Date: 11/1/2022
Primary Author: CIO & AVP of Information Technology

General Description

Purpose:

The purpose of this policy is to safeguard CSUB computer systems in a manner that will ensure the confidentiality integrity and availability of the data maintained on them. This policy addresses the default security state of any system being deployed and ensures that only needed services and functions are installed and enabled by default.

The method used by the California State University Chancellor's offices and the California National Guard in their audits is to utilize a product offered by the Department of Defense called Security Content Automation Protocol (SCAP)

Definition:

- SCAP - Security Content Automation Protocol: Department of Defense provided tool that evaluates the security of a computer system configuration by checking against a set standard security template CCE that is also provided by the DOD to provide a baseline score.
- CCE - Common Configuration Enumeration: a comprehensive list of identifiers for common and uncommon system configuration issues
- SCAP Score- a numeric score from one to 100 provided by the SCAP tool. Hosts with a lower SCAP Score are typically more easily exploited by threat actors.

Scope:

The policy will apply to all California State University Bakersfield managed state-owned computer devices, including workstations, and servers including auxiliaries.

Policy/Procedure

All devices utilized by the campus must meet a minimum SCAP Score as set forth by the Information Security Officer.

- Servers must meet a minimum SCAP Score of **70.00%**
- Workstations must meet a minimum SCAP Score of **70.00%**
- All base images must be verified by running the SCAP tool after any update or change, to ensure they remain in compliance with this policy.
- The Information Technology Services Infrastructure team will spot check 5 random existing servers annually and report their findings to the Deputy Chief Information Officer and Information Security Officer no later than November 1st of every year.
- The Information Technology Support Services team will spot check 10 random existing workstations annually and report their findings to the Director of Support Services and Information Security Officer no later than November 1st of every year.
- Any server or workstation that is not compliant with this policy must receive a written exception from the Information Security Officer prior to deployment.

Review (Frequency and Process)

This policy shall be reviewed every two years by the Information Security Officer and provided to the Associate Vice President & CIO for approval.

Related Documents

Related Content:

Department of Defense Security Content Automation Protocol Resources:
https://public.cyber.mil/stigs/scap/