System Hardening

NIST Standards and other best practices.

NIST 800-53r5 – IA-2 – Identification and Authentication (Organizational Users)

NIST 800-82r3 – 6.2.1.4 .4. – Multi-Factor Authentication

The background material for this scenario discusses the use of multi-factor authentication.

NIST 800-53r5 – IA-5 – Authenticator Management

NIST 800-82r3 – 6.2.1.4.5. – Password Authentication

The lab associated with this scenario demonstrates the importance of selecting secure passwords that are not found in password dictionaries.

NIST 800-53r5 – SI-2 – Flaw Remediation

NIST 800-82r3 – 6.2.11. – Flaw Remediation and Patch Management

NIST SP 800-40, Rev. 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology

Students demonstrate in the lab some of the negative results that can occur if systems are not patched promptly.

NIST 800-53r5 – CM-7 – Least Functionality

NIST 800-82r3 – 5.2.5.4. – Configuration Management

NIST 800-82r3 – 6.2.4.1. – Least Functionality

The students will demonstrate the danger of leaving unnecessary services running when completing the lab associated with this scenario.

NIST 800-53r5 – SC-7 (12) – Boundary Protection – Host-Based Protection

NIST 800-82r3 – 5.2.3.1. – Network Architecture

NIST 800-123 – 4.3 – Install and Configure Additional Security Controls

The background material associated with this lab discusses host-based security software such as anti-virus, firewalls and logging. The lab used with this scenario demonstrates the importance of implementing a host-based firewall.