

Instructional Scenario

Inside Operating System Security



Course/Duty Area: Cybersecurity Fundamentals/Securing Operation Systems

Scenario:

A mid-sized organization operating across multiple sectors—including finance, healthcare, and logistics—has identified operating system security as a critical weakness following a recent security assessment. While no major breach has occurred, the assessment revealed outdated operating systems, inconsistent patching practices, misconfigured user permissions, and limited use of virtualization for testing and isolation. As a systems security technician, you are tasked with evaluating the organization's operating systems and recommending improvements. You must understand how operating systems function, identify vulnerabilities and threats that target operating systems, and apply best practices to harden systems while maintaining reliability and performance. You will explore multiple operating systems, evaluate security settings, analyze logs, and use virtualization to safely test configurations and security controls.

Big Question:

How can securing operating systems reduce organizational risk while ensuring systems remain functional, reliable, and available?

Focused Questions:

- What are the primary functions of an operating system (OS), and how do they support applications and users?
- How do different operating systems (Windows, Linux, macOS, mobile) vary in structure and security features?
- What vulnerabilities and threats commonly target operating systems?
- How do patch management, updates, and system hardening reduce risk?
- Why are authentication, access control, and auditing critical OS security parameters?
- How do logs, backups, and virtualization support secure system operations?

Student Project or Outcome:

Students will work individually or in teams to complete an Operating System Security Evaluation for the organization. They will analyze one or more operating systems, identify risks, and recommend security improvements aligned to industry's best practices.

Project-Based Assessment:

Operating System Hardening Plan (Primary Assessment)

Students act as systems security technicians tasked with hardening an operating system used by the organization.

Project Deliverables

- Identification of the selected operating system and its role
- Overview of core OS components and functions
- Identification of common OS vulnerabilities and threats

- Step-by-step OS hardening recommendations (patching, updates, service management)
- Explanation of how hardening improves confidentiality, integrity, and availability

Format Options: Written hardening guide, checklist, or slide presentation

Alternative Projects:

OS Vulnerability and Exploit Case Study

Students research a real-world operating system vulnerability or exploit and analyze its impact.

Project Deliverables

- Description of the vulnerability or exploit (e.g., zero-day, privilege escalation, rootkit)
- Operating system(s) affected
- How the vulnerability is exploited
- Potential organizational impact
- Recommended mitigation strategies (patches, configuration changes, controls)

Format Options: Case study report, infographic, or analyst brief

Authentication, Access Control, and Audit Policy Review

Students evaluate critical operating system security parameters.

Project Deliverables

- Review of authentication mechanisms (passwords, MFA, accounts)
- Analysis of access control and permissions
- Overview of audit and logging policies
- Identification of weaknesses and recommendations for improvement

Format Options: Policy review document or briefing presentation

Logs, Backups, and Incident Readiness Project

Students explore how operating systems support detection, recovery, and resilience.

Project Deliverables

- Explanation of OS security and audit logs and their purpose
- Description of backup types and locations
- Discussion of how logs and backups support incident response and recovery
- Example incident scenario showing how logs or backups would be used

Format Options: Report, scenario write-up, or visual diagram

Virtualization and Sandbox Security Lab

Students explore virtualization as a security tool for testing and isolation.

Project Deliverables

- Explanation of virtualization concepts and key properties (Task 94)
- Comparison of containers, hypervisors, and hyperscale's
- Description of how virtual machines can be used as sandboxes
- Advantages and disadvantages of virtualization for security

Format Options: Lab report, comparison chart, or presentation

Teacher Resources:

- [Virginia Cyber Range](#)
- [NIST Cybersecurity Framework](#)
- [Common Vulnerabilities and Exposures \(CVE\) Database](#)
- [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)

- **NIST Security Configuration Baselines & Publications**
Authoritative guidance for operating system security, configuration baselines, and system hardening
 - [NIST Computer Security Resource Center \(CSRC\)](#)
 - [NIST Special Publications: SP 800 series \(guidance\)](#)
 - [NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations](#)

- **Operating System Hardening Guides**
Practical, real-world hardening references for Windows and Linux systems
 - [CIS Benchmarks List](#), Center for Internet Security
 - [Microsoft cloud security benchmark documentation](#)
 - Linux Security Hardening Guides: [Ubuntu](#) and [General Linux](#)

- **Virtualization Tools and Documentation**
Tools commonly used to explore sandboxing, isolation, and virtualization security
 - [Oracle VirtualBox](#)
 - [VMware Workstation Player](#)
 - [Microsoft Hyper-V Overview](#)
 - [Docker \(Containers\)](#)

Scenario submitted by Kristi Rice, Spotsylvania High School, Spotsylvania County Public Schools