
# Systems Hardening and Cybersecurity

Ammar Yasser Mohamed
Course Code: ONL3_ISS2_S2
23 July 2025

## 1 What is Systems Hardening?

Systems hardening is all about tightening the security of a computer system by removing potential entry points for attackers. This includes disabling unused services, getting rid of outdated software, applying updates and patches, and sticking to recommended security settings. The main idea is to reduce the system's "attack surface"—in other words, to minimize the ways in which it could be exploited.

**Why It Matters:** Hardening is a proactive step in cybersecurity. Rather than waiting for an attack to happen, it's about preparing in advance—making systems tougher to break into. This helps reduce the chances of breaches, malware infections, and unauthorized access.

### Which Systems Benefit from Hardening?

- **Servers:** Since servers store and process critical data, they're often high-value targets. Hardening ensures they're better protected from cyber threats.
- **Workstations:** Even regular computers used by staff or students can be vulnerable. Hardening them helps prevent malware infections and phishing attacks.
- **Network Devices:** Routers, firewalls, and switches are vital for communication between systems. If compromised, they could allow attackers into an entire network.

That's why they need hardening, too.

# 2 Common Techniques for Systems Hardening

## 1. Disabling Unnecessary Services

Many systems come with default services running in the background—even ones that aren't being used. These can create unnecessary vulnerabilities. Turning off unused services reduces risk and improves overall performance.

## 2. Least Privilege Access

The principle of least privilege means giving users only the access they truly need—nothing more. If a user's account is hacked, limiting its permissions can stop attackers from doing major damage.

## 3. Patch Management

Software vendors frequently release updates to fix security flaws. By regularly installing these patches, systems stay protected against known vulnerabilities. Ignoring updates is like leaving your front door open.

## 4. Configuration Baselines

A configuration baseline is a set of standard, secure settings that systems should follow. This makes it easier to set up new devices securely and detect changes that might signal a security issue.

## 5. Network Segmentation

Rather than having one big network where everything is connected, it's better to divide it into smaller zones. If a threat gets into one part, it won't easily spread to the rest. This method also allows more control over who can access what.

# 3 Security Standards and Guidelines That Support Hardening

## CIS Benchmarks

The Center for Internet Security (CIS) offers detailed guides on how to secure various systems. These benchmarks are widely respected and provide clear, step-by-step instructions for hardening everything from operating systems to cloud environments.

## NIST Guidelines

The National Institute of Standards and Technology (NIST) is a U.S. agency that provides frameworks and special publications like SP 800-53. These offer comprehensive guidelines on how to secure federal systems—and are also useful for private organizations.

## ISO/IEC 27001

This international standard focuses on managing information security as a whole. While it's more about policies and risk management, it includes practices that support system hardening, such as asset control and access management.

## Why These Standards Matter

Following standards like CIS, NIST, or ISO helps organizations build consistent, secure systems. They also help meet legal and regulatory requirements, and can improve readiness in case of a cybersecurity incident. Most importantly, they provide a reliable roadmap for keeping systems hardened and safe.