

# Security hardening Wrap-up & Glossary terms from week 4

Great work on learning about security hardening!  
Let's take a few minutes to wrap up what you've learned.

You learned about security hardening and its importance to an organization's infrastructure. First, we discussed how security hardening strengthens systems and networks to reduce the likelihood of an attack.

Next, we covered the importance of OS hardening, including patch updates, baseline configurations, and hardware and software disposal.

Then we explored network hardening practices, such as network log analysis and firewall rule maintenance.

Finally, we examined cloud network hardening and the responsibilities of both organizations and cloud service providers in maintaining security.

As a security analyst, you'll be working with operating systems, on-premise networks, and cloud networks.

You'll be using all the knowledge that we learned in this section in your career as a security analyst.

## Terms and definitions from Course 3, Week 4

**Baseline configuration (baseline image):** A documented set of specifications within a system that is used as a basis for future builds, releases, and updates

**Hardware:** The physical components of a computer

**Multi-factor authentication (MFA):** A security measure which requires a user to verify their identity in two or more ways to access a system or network

**Network log analysis:** The process of examining network logs to identify events of interest

**Operating system (OS):** The interface between computer hardware and the user

**Patch update:** A software and operating system update that addresses security vulnerabilities within a program or product

**Penetration testing (pen test):** A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes

**Principle of least privilege:** Access and authorization to information only last long enough to complete a task

**Security hardening:** The process of strengthening a system to reduce its vulnerabilities and attack surface

**Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities for an organization

**World-writable file:** A file that can be altered by anyone in the world

---

Revision #3

Created 3 July 2023 10:37:47 by naruzkurai

Updated 3 July 2023 10:39:42 by naruzkurai