Hardening Linux and Windows servers according to CIS and STIG

Course code: LXHARD

In this four-day course, participants will gain both theoretical and practical skills in applying CIS and STIG recommendations, auditing, and automating hardening (Ansible, SCAP tools).

Who is the course for

IT administrators, security specialists, DevOps/SecOps engineers.

What you will learn

- Understand the principles of CIS and STIG, their differences, and practical application.
- Gain the ability to manually and automatically harden Linux and Windows servers.
- Develop skills in using audit tools (OpenSCAP, CIS-CAT, STIG Viewer / SCAP).
- You will have a ready-made Ansible playbook for hardening and reporting scripts.

Prerequisite knowledge

Basic Linux and Windows administration (working with the command line, basic GPO/AD knowledge).

Course materials

Presentations, PDF outlines, VM images/virtual machines, sample scripts and playbooks, participation certificate.

Course outline

- Introduction + CIS for Linux &Windows
- Introduction to hardening: principles (attack surface minimization, least privilege), common threats and regulations (PCI DSS, NIST).
- Overview of CIS Benchmarks: structure, Level 1 vs Level 2, how to obtain and read the benchmark.
- Examples of CIS recommendations for Linux and Windows (accounts, services, logging, network).
- Practical exercise: analysis of CIS Benchmark (e.g., Ubuntu and Windows Server) and demo scanning (CIS-CAT Lite/Pro).
- STIG, comparison of STIG vs CIS + tools
- Introduction to STIG (DISA, CAT I-III), SCAP, differences compared to CIS, and when to use each standard.
- Working with STIG Viewer and SCAP tools, demo SCAP/OSCAP scanning.
- Group activity: comparing a specific rule (e.g., password policy) in CIS vs STIG.
- Hands-on: Hardening Linux
- Kernel &sysctl, systemd services, firewall (firewalld/ufw), file permission management, SELinux/AppArmor.
- Examples of CIS and STIG rules for Linux (explanation and impact).
- Practical lab: manual hardening of Ubuntu/RHEL according to CIS Level 1; implementation of selected STIG CAT I rules.
- Compliance verification: OpenSCAP / CIS-CAT scanning and result interpretation.
- Hands-on: Windows Hardening + Ansible Automation
- Hardening Windows Server (Group Policy, registry, firewall, Windows Defender), CIS and STIG examples (SMBv1, audit, ACL).
- Introduction to Ansible (inventory, playbooks) + overview of CIS/STIG roles and WinRM for Windows.
- Workshop: creating and running Ansible playbooks — Linux and Windows hardening.
- Final project: deploy the playbook and verify compliance (CIS-CAT / OpenSCAP).