13th International Conference on Applied Informatics
Eszterházy Károly Catholic University
Eger, Hungary, February 19–21, 2026

Comparative Analysis of Vulnerability Dynamics in Operating Systems and Containerized Environments

Ferenc Koczka

[a]Eszterhazy Karoly Catholic University
koczka.ferenc@uni-eszterhazy.hu

Abstract

One of the most significant challenges in modern IT infrastructure management is maintaining the delicate equilibrium between technical debt and security integrity. In environments characterized by rapidly evolving requirements, research and economic priorities often necessitate the deployment of ad-hoc solutions. This process typically results in significant heterogeneity, where legacy systems and sub-optimally configured endpoints coexist.

The central hypothesis of this research is that the "freshly installed" state of an operating system—even with a minimal package selection—does not, in itself, constitute a guarantee of security. This study performs a comparative analysis of the security profiles of traditional, monolithic operating system installations versus modern, Proxmox-based containerized solutions, with specific regard to the vulnerability lifecycle and the recommendations of the CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology).

Theoretical Framework and Regulatory Environment

The theoretical foundation of this study is provided by international cybersecurity frameworks that define system protection levels in quantifiable terms:

- NIST SP 800-53 (SI-2 – Flaw Remediation): Protocols for proactive management of security defects throughout the system lifecycle.

- NIST SP 800-53 (SC-7 – Boundary Protection): Requirements for logical isolation and service segmentation.
- NIST SP 800-190 (Application Container Security Guide): A specialized architectural security guide for containers, which notes that while containers natively offer a reduced attack surface, they introduce specific risks, such as shared kernel vulnerabilities.
- CIS Ubuntu Linux 24.04 LTS STIG Benchmark: A collection of industry best-practice configuration parameters for system hardening.
- CVSS (Common Vulnerability Scoring System): An objective metric system used to determine the severity of software vulnerabilities.

Methodology and Data Collection

The research is divided into two phases. The first phase involved a retrospective analysis conducted within university network environments, which was subsequently expanded in the second phase to include the infrastructures of commercial enterprises with over 50 employees.

The empirical investigation focused on the correlation between the age of systems and the quantity and severity of identified critical defects. Technical validation was performed using the Wazuh open-source SIEM and XDR platform, enabling real-time vulnerability detection and configuration auditing. Experimental Setup:

- Reference Group: Ubuntu 24.04 LTS operating system configured with default settings.
- Test Group: An LXC container running in a Proxmox VE environment, providing functionally equivalent services to the reference system.

The assessment utilized network and local scanning protocols to monitor the following parameters:

- Number and nature of open ports and exposure surfaces.
- Redundancy of active daemon processes.
- Presence of well-known vulnerabilities (CVEs).
- Deviations from CIS configuration recommendations (Hardening Drift).

Results

The measurements confirmed the phenomenon of vulnerability entropy: as uptime increases, system configurations inevitably drift away from the secure baseline

(configuration drift), while the number of accumulated unpatched defects shows an exponential trend.

Data revealed that an "out-of-the-box" installation fulfills only approximately 40 percent of the CIS benchmark requirements. In contrast, the tactical superiority of containerized environments rests on three pillars:

Architectural Minimalism: Due to the abstraction level of container images, unnecessary hardware interactions and kernel modules are absent, significantly reducing the attack surface.

Logical Isolation: Namespace isolation and resource partitioning (cgroups) effectively restrict lateral movement in the event of a compromise.

Immutability: The container-based approach supports the "Immutable Infrastructure" concept, where systems are redeployed rather than patched, ensuring continuous compliance with the NIST SP 800-53 SI-2 control.

Conclusion

The research demonstrates that vulnerability management is not merely an operational maintenance task but a critical architectural decision. To enhance the security integrity of systems, the following strategic guidelines are proposed:

Modernization Strategy: Prioritizing containerized migration for legacy, monolithic systems rather than traditional in-place upgrades.

Hardening by Default: Utilizing Proxmox-based templates that incorporate CIS-specific hardening at the moment of instantiation.

Auditability: Versioned images facilitate the automation and traceability of change management and NIST-compliant auditing.

In summary, the implementation of container technology within the Proxmox ecosystem results not only in operational efficiency but also in a significant and measurable reduction of cybersecurity risks compared to traditional architectures.

References

[1] Center for Internet Security: *CIS Benchmarks: Ubuntu Linux 24.04 LTS STIG Benchmark*, URL: https://www.cisecurity.org/cis-benchmarks (visited on 01/29/2026).

[2] FIRST.org, Inc.: *Common Vulnerability Scoring System (CVSS)*, URL: https://www.first.org/cvss/ (visited on 01/29/2026).

[3] O. Jarkas et al.: *A Container Security Survey: Exploits, Attacks, and Defenses*, ACM Computing Surveys 57.7 (2024), DOI: 10.1145/3715001.

[4] Jumiaty, B. Soewito: *SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive*, International Journal of Advanced Computer Science and Applications 15.9 (2024).

[5] National Institute of Standards and Technology: *Special Publication 800-190: Application Container Security Guide*, 2017, URL: https://csrc.nist.gov/pubs/sp/800/190/final (visited on 01/29/2026).

[6] S. Stanković, S. Gajin, R. Petrović: *A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis*, in: Proceedings of the IX International Conference, 2024.