From Attack to Defense: Incident Response and Threat Mitigation on Linux Systems

Elnur Mammadov
ADA University, Baku, Azerbaijan

Vusal Abbasov
ADA University, Baku, Azerbaijan

Nicat Osmanli
ADA University, Baku, Azerbaijan

Abstract:

In the modern cybersecurity landscape, organizations face increasingly sophisticated attacks that require efficient incident response and strong threat mitigation strategies. Linux systems play a critical role in cybersecurity operations due to their flexibility, security features, and widespread use in enterprise environments.

In this study, we explore how Linux systems are utilized across different stages of cybersecurity operations, from attack detection to response and mitigation. We examine common attack vectors targeting Linux environments, including misconfigurations, unauthorized access, and network-based threats.

The paper further focuses on practical defensive techniques, such as intrusion detection, log analysis, firewall configuration, and system hardening. Additionally, we demonstrate how incident response procedures can be implemented using native Linux tools and commands.

By combining system administration knowledge with cybersecurity practices, this work provides a practical perspective for students and early-career professionals aiming to apply Linux skills in real-world security scenarios.