Techniques for Hardening Systems

▼ 1. Disabling Unnecessary Services

> Disabling unnecessary services involves turning off or removing software, applications, and services that are not essential to a system’s function. Many operating systems come with various default services that can be exploited by attackers if left enabled, particularly if these services have known vulnerabilities.

> Reducing active services limits the system's "attack surface," or the number of potential entry points that attackers could exploit. When non-essential services are disabled, the likelihood of unauthorized access or system exploitation decreases. Additionally, disabling these services reduces system resource consumption, enhancing performance and stability. This is a fundamental hardening technique because every enabled service represents a possible vulnerability.

▼ 2. Implementing Least Privilege Access

> The principle of least privilege restricts users’ and applications’ permissions to only those necessary to perform their functions. This means each user or application is granted the minimum access rights necessary and nothing more. For example, standard

employees might not have administrative rights, while administrators have access only to areas they are responsible for managing.

Enforcing least privilege access minimizes the impact of a security breach. If a cyber attacker gains access through a compromised account, their actions will be limited by the account's restricted permissions, which can prevent significant damage. It reduces the risk of data exposure and unauthorized changes to critical configurations, making it harder for attackers to escalate privileges or move laterally across the system.

▼ 3. Patch Management

Patch management is the process of routinely updating software and firmware to fix known security vulnerabilities and bugs. This includes applying patches provided by software vendors for operating systems, applications, and hardware devices.

Keeping systems up-to-date with the latest patches closes vulnerabilities that attackers could exploit. Patch management is crucial because cybercriminals often target known vulnerabilities soon after they are disclosed. Regular patching ensures that systems are protected against the latest threats, improving the overall security posture and reducing the risk of successful exploits.

▼ 4. Configuration Baselines

Configuration baselines establish a standardized security configuration for all systems, setting predefined security

> policies and configurations to ensure consistency across the network. Baselines cover various settings, including user permissions, access controls, and network configurations.

> Configuration baselines improve security by ensuring that all systems adhere to a standard level of protection. This minimizes misconfigurations, which are a common cause of security vulnerabilities. By defining and enforcing secure configurations, configuration baselines reduce variability, making it easier to manage security across multiple systems and to identify and correct deviations that could introduce risks.

▼ 5. Network Segmentation

> Network segmentation divides a network into smaller, isolated segments to control traffic flow between them. It enables organizations to separate sensitive or critical areas (like financial data servers) from less critical ones, often using firewalls or virtual local area networks (VLANs) for enforcement.

> Network segmentation limits an attacker's ability to move freely within a network if they manage to breach one segment. Isolating critical assets minimizes exposure to threats, making it harder for attackers to reach valuable data or gain control of essential systems. Segmentation also improves monitoring by reducing "noisy" network traffic, allowing security teams to more easily detect and respond to suspicious activity.