Session 2 Assignment: 2. Techniques for Hardening Systems

Techniques for Hardening Systems:

To protect systems against cyber threats, a range of hardening techniques can be applied to reduce vulnerabilities and prevent unauthorized access.

Here are five commonly used systems hardening techniques:

1. Disabling Unnecessary Services

Security Contribution: By disabling unnecessary services, the system reduces its exposure to vulnerabilities that could be exploited by attackers. Each active service presents a potential entry point for cyberattacks, especially if they contain security flaws.

By removing or disabling these services, the system's attack surface is minimized, making it more challenging for an attacker to exploit any weaknesses. Additionally, fewer active services help simplify monitoring and reduce the burden on system resources, improving overall system performance and resilience.

2. Implementing Least Privilege Access

Security Contribution: Implementing least privilege access limits the potential impact of compromised accounts by restricting what users can do. If an account with limited privileges is compromised, the attacker's access is similarly restricted, preventing them from accessing critical systems or sensitive information. This technique also reduces the risk of accidental or intentional misuse of permissions by internal personnel, protecting sensitive data and enhancing overall security by containing the scope of access.

3. Patch Management

Security Contribution: Effective patch management ensures that systems remain protected against known vulnerabilities. Failing to apply patches leaves systems exposed to cyber threats that exploit outdated software. Keeping software and systems up-to-date minimizes the risk of attacks that take advantage of unpatched vulnerabilities, such as ransomware or zero-day exploits. Moreover, automated patching policies can improve response times to new threats, maintaining the integrity and security of the entire IT infrastructure.

4. Configuration Baselines

Security Contribution: By establishing and enforcing configuration baselines, organizations can ensure that all systems are set up according to best practices, reducing the likelihood of configuration errors or insecure setups. Consistent baselines across systems help prevent unauthorized changes and ensure each system is configured to meet security standards. Furthermore, monitoring systems against baselines helps detect and correct deviations, mitigating the risks of misconfigurations that could lead to security breaches.

5. Network Segmentatio

Security Contribution: Network segmentation limits the movement of attackers within a network. In a segmented network, even if one segment is breached, the attacker's access is restricted, preventing lateral movement to other critical areas. This technique is especially valuable in protecting sensitive data or systems, such as payment information or internal databases, by placing them in isolated segments with stricter access controls. Segmentation also allows for tailored security policies per segment, enhancing the overall security posture of the network.