A Disturbing Discovery

Week Two at Pandora Company Limited

Name :- Nonis S.S.L Index No :- 210439P

Pandora Company Limited's current server environment is vulnerable due to default operating system configurations on its Rocky Linux 9 and Windows Server 2019 R2 servers. This report addresses these risks by applying trusted security hardening frameworks like CIS benchmarks. By enhancing key areas like file permissions, service settings, and user management, the recommended measures will significantly strengthen Pandora's overall security posture.

Identifying a Reputed Hardening Framework

Center for Internet Security (CIS) Benchmarks are widely trusted for providing security hardening guidance for various platforms, including Linux and Windows. CIS benchmarks provide prescriptive guidance for securing system configurations against common vulnerabilities. The CIS Level 1 and Level 2 benchmarks are practical for implementing and meeting industry best practices.

Rocky Linux 9 :-

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for Rocky Linux. We can use the CIS_Rocky_Linux_9_Benchmark_v2.0.0 benchmark for this.

Windows Server 2019 R2 :-

CIS provides a specific benchmark for Windows Server 2019, and it's an excellent starting point for hardening Windows environments. The benchmark is CIS_Microsoft_Windows_Server_2019_Benchmark_v3.0.1

Identify Key Hardening Sections

- Filesystem Configurations
- Service Settings
- User and Account Management
- Logging and Monitoring
- Firewall and Network Configurations
- Patch Management
- Secure Boot and Kernel Hardening

Windows Server 2019 R2: Improvements over Default Settings

a) **Filesystem Configurations:**

- **Default Settings:** Basic filesystem permissions are applied, and default encryption settings like BitLocker may be disabled. Volume Shadow Copy is enabled by default for backups, which can expose sensitive data.
- **Recommended Settings:** Implement encryption for sensitive directories (using BitLocker or other encryption mechanisms) and ensure the proper use of access control lists (ACLs) for managing permissions.
- **Security Implications:** Encrypting sensitive data helps protect it from unauthorized access, especially in the event of physical theft or system compromise. By using ACLs, permissions can be restricted to only authorized users, minimizing exposure to internal or external threats.

b) **Service Settings:**

- **Default Settings:** Services are set to start automatically by default, including many that may not be needed.

- **Recommended Settings:** Disable unnecessary services or set them to "Manual" startup, ensuring that only essential services are running.
- **Security Implications:** Reducing the number of active services minimizes potential vulnerabilities and entry points for attackers, decreasing the attack surface and improving system stability.

c) **Account Policies:**
- **Default Settings:** Default password policies are weak, with minimum requirements for password complexity and length. Account lockout thresholds are not adequately configured, making the system more susceptible to brute-force attacks.
- **Recommended Settings:** Enforce stronger password policies (14+ characters, complexity requirements), account lockout policies, and implement multi-factor authentication (MFA).
- **Security Implications:** Stronger password policies reduce the risk of password cracking, while MFA provides an additional layer of security against unauthorized access. Properly configured account lockout thresholds further deter brute-force attacks.

d) **Local Policies:**
- **Default Settings:** Default audit policies log only minimal activity, and Remote Desktop Services may be enabled by default, increasing the risk of remote attacks.
- **Recommended Settings:** Enhance logging and auditing policies, secure remote desktop access with strong authentication, and configure firewalls to block all incoming traffic by default.
- **Security Implications:** Strengthening audit policies ensures more comprehensive tracking of system activity, allowing for quicker detection of suspicious events. Securing remote access and limiting traffic to authenticated users reduces the risk of unauthorized access.

e) **Logging and Monitoring:**
- **Default Settings:** Basic logging is enabled, but it is not comprehensive enough to detect and address potential security incidents.
- **Recommended Settings:** Implement advanced logging configurations and regularly review logs for any signs of unauthorized access or suspicious behavior.
- **Security Implications:** Comprehensive logging allows administrators to detect, respond to, and mitigate potential security incidents more effectively.

f) **Firewall Configuration:**
- **Default Settings:** The default configuration allows incoming connections from trusted networks but may not be optimized for security.
- **Recommended Settings:** Implement custom firewall rules, enable logging, and define VPNs and Intrusion Prevention Systems (IPS).
- **Security Implications:** Customized firewall rules ensure better control over incoming and outgoing traffic. Logging and VPNs provide secure access, while IPS actively defends against network-based attacks.

g) **Advanced Audit Policy Configuration:**
- **Default Settings:** Basic audit settings may not monitor key system events, such as credential validation.
- **Recommended Settings:** Enable advanced auditing for both successful and failed login attempts and security-critical events.
- **Security Implications:** Detailed auditing enables the detection of failed access attempts or abnormal behavior, which can help mitigate security incidents in real-time.

Rocky Linux 9:

a) **Filesystem Configurations:**
   - **Default Settings:** The default filesystem configuration lacks encryption, and the root partition contains all data. Sensitive directories like /var, /tmp, and /home may not be segregated.
   - **Recommended Settings:** Create separate, encrypted partitions for sensitive directories, apply stricter permissions, and schedule regular filesystem checks.
   - **Security Implications:** Encrypting sensitive directories and using stricter permissions reduces the risk of unauthorized access while segregating partitions and scheduling regular checks enhances data integrity and system reliability.

b) **Service Settings:**
   - **Default Settings:** Services may run with default configurations, potentially exposing unnecessary services.
   - **Recommended Settings:** Disable or limit the use of non-essential services, adjusting startup types to "Manual" where applicable.
   - **Security Implications:** Limiting unnecessary services reduces exposure to vulnerabilities, freeing up system resources and improving overall performance.

c) **User and Account Management:**
   - **Default Settings:** Users may have broad permissions by default, and access control may be weak.
   - **Recommended Settings:** Implement least privilege principles, enforce SE-Linux, and regularly audit user accounts.
   - **Security Implications:** Enforcing the least privilege ensures that users only have the minimal required access, reducing potential misuse of privileges. Regular audits help maintain tight control over account management.

d) **Logging and Monitoring:**
   - **Default Settings:** Basic logging configurations are applied by default but may not capture comprehensive security data.
   - **Recommended Settings:** Configure advanced logging to capture detailed security-related events, such as file access and authentication attempts.
   - **Security Implications:** Enhanced logging enables quick detection of potential threats, ensuring swift action and mitigation.

e) **Firewall Configuration:**
   - **Default Settings:** The default Firewall configuration allows certain types of traffic by default, potentially exposing unnecessary services.
   - **Recommended Settings:** Block all incoming traffic by default and allow only explicitly required connections.
   - **Security Implications:** Reducing the number of exposed services and implementing stricter firewall rules significantly lowers the system's attack surface.

f) **Advanced Security Policies:**
   - **Default Settings:** Basic security policies may not provide adequate protection against sophisticated threats.
   - **Recommended Settings:** Enable SE-Linux and App-Armor to enforce granular access control policies and configure secure boot processes.
   - **Security Implications:** These measures add multiple layers of security, protecting the system against advanced persistent threats and other sophisticated attacks.

Proposal for Implementation for Future Server Installations

Pandora Company Limited should follow these hardening steps to enhance the security of its infrastructure,

Rocky Linux 9:

- Implement encrypted partitions for sensitive data, disable unnecessary services, enforce strict access control measures, improve system logging, and ensure that the system regularly applies updates to protect against vulnerabilities.

Windows Server 2019 R2:

- Strengthen account policies by enforcing complex passwords and limiting login attempts, minimizing the number of active services to reduce the attack surface, customizing firewall rules to control traffic, implementing advanced auditing policies for tracking system events, and securing system settings to protect against unauthorized changes.

Summary

Implementing the recommended hardening measures will significantly strengthen Pandora Company Limited's security posture. By mitigating vulnerabilities in default configurations, the company will minimize its attack surface, bolster system resilience, and enhance protection against evolving cyber threats. This proactive approach will improve the overall security of their Linux and Windows environments, ensuring a robust defense against potential exploits.

References

- CIS_Rocky_Linux_9_Benchmark_v2.0.0
  https://www.cisecurity.org/benchmark/rocky_linux
- CIS_Microsoft_Windows_Server_2019_Benchmark_v3.0.1
  https://www.tenable.com/audits/CIS_Microsoft_Windows_Server_2019_v3.0.1_NG_MS
- CIS Benchmarks - CIS Center for Internet Security