Week Two at Pandora Company Limited

A Disturbing Discovery

Name: Lahiru Randika **Index : 210527J**

1. Introduction

Pandora Company Limited has been identified with significant security risks due to default operating system configurations on its servers. This report addresses these vulnerabilities by recommending a security hardening framework and providing a structured plan to enhance the security posture of the company's IT infrastructure.

Here I have chosen the Center for Internet Security benchmarks to do this hardening process, and the Introduction for CIS is mentioned under the topic of "Identifying Reputed Hardening Framework".

2. Identifying a Reputed Hardening Framework

The Center for Internet Security (CIS) benchmarks is a widely recognized and trusted framework for security hardening across various operating systems, including Rocky Linux and Windows Server. CIS benchmarks provide prescriptive guidance for securing system configurations against common vulnerabilities. The CIS Level 1 and Level 2 benchmarks are practical to implement and meet industry best practices.

Rocky Linux 9:

- ✓ Framework: Center for Internet Security (CIS) Benchmarks
- ✓ Benchmark: CIS_Rocky_Linux_9_Benchmark_v2.0.0

Windows Server 2019 R2:

- ✓ Framework: Center for Internet Security (CIS) Benchmarks
- ✓ Benchmark: CIS_Microsoft_Windows_Server_2019_Benchmark_v3.0.1

These frameworks are globally recognized for their comprehensive guidelines on securing operating systems and are well-suited for the systems in use at our Pandora Company Limited.

3. Categorizing Key Hardening Sections and Analyzing

For both Rocky Linux 9 and Windows Server 2019 R2, the primary areas addressed by the hardening guidelines include:

1. **Filesystem Configurations**
2. **Service Settings**
3. **User and Account Management**
4. **Logging and Monitoring**
5. **Firewall Configuration**
6. **Advanced Security Policies** and more.

Windows Server 2019 R2

1. Filesystem Configurations:

- **Default Settings:**
  - Basic filesystem permissions are applied by default.
  - Volume Shadow Copy Service is enabled by default for creating backups and volumes.
  - Default encryption schemas like BitLocker (In most cases disabled)
- **Recommended Settings:**

- Implement encryption for sensitive directories and secure filesystems with appropriate permissions.
- Implement least privilege by restricting permissions to only those necessary for users and processes. Use access control lists (ACLs) to manage permissions more granularly.
- Regular backups and enable secure encryption system.

- **Security Implications:**

Implementing encryption for sensitive directories protects data from unauthorized access, while securing filesystems with appropriate permissions reduces the risk of data breaches. Restricting permissions and using ACLs ensures that only authorized users and processes have access, minimizing potential attack vectors. Regular backups combined with encryption safeguard against data loss and theft, enhancing overall security and data integrity.

2. Service Settings:

- **Default Settings:**
  - Services are typically set to "Automatic" by default.
- **Recommended Settings:**
  - Change startup types of non-essential services to "Manual" or "Disabled" based on their necessity.
- **Security Implications:**

Reducing the number of running services minimizes potential entry points for attackers, optimizing system stability and security.

3. Account Policies:

- **Default Settings:**
  - Password Policy: Minimum 7 characters on domain members and 0 characters on stand-alone servers, 24 passwords remembered on domain members and 0 passwords remembered on stand-alone servers, 42-day maximum age.
  - Account Lockout Policy: 0 failed attempts threshold, None or 30-minute lockout duration, None or 30 minutes reset account lockout counter after (if Account lockout threshold is configured).
  - Kerberos Policy: 10-hour maximum token lifetime.
- **Recommended Settings:**
  - Increase password length to 14 or more characters and enable complexity requirements.
  - The recommended state for password history is 24 or more passwords.
  - The recommended state for maximum password age is 365 or fewer days, but not 0.
  - Set account lockout threshold to 5 or fewer invalid login attempt(s), but not 0.
  - Implement multi-factor authentication (MFA) and strong encryption methods (Also should disable the reversible encryption methods).
  - Regularly monitor and audit security events.
- **Security Implications:**

Implementing a password length of 14 or more characters and enforcing complexity requirements significantly enhances account security by making passwords harder to crack. Enforcing a password history of 24 or more prevents users from reusing old passwords, reducing the risk of recurring vulnerabilities. Limiting the maximum password age to 365 days or fewer ensures regular updates, keeping accounts secure from long-term password exposure. Setting an account lockout threshold of 5 or fewer invalid attempts reduces brute force attack risks. Finally, multi-factor authentication (MFA) and strong encryption methods, combined with regular monitoring and auditing, add robust layers of defense, ensuring account integrity and immediate response to suspicious activities.

4. Local Policies:

- **Default Settings:**

- Audit object access (default: Access this computer from the network or by pre-defined authorized parties), account logon/logoff, policy changes.
- Remote Desktop Services are Disabled by default.

- **Recommended Settings:**
  - Configure Windows Firewall to block all incoming traffic by default.
  - Allow only administrators and authenticated parties to access it from the network.
  - Use a password management tool for enforcing strong passwords.
  - Secure remote desktop access with strong authentication methods.
- **Security Implications:**

Configuring Windows Firewall to block all incoming traffic by default ensures that only necessary and explicitly allowed connections are made, reducing the attack surface. Limiting access to the firewall configuration to administrators and authenticated users prevents unauthorized changes, securing the system from internal or external threats. Using a password management tool enforces strong, unique passwords, reducing the likelihood of weak passwords being exploited. Securing remote desktop access with strong authentication methods, such as multi-factor authentication (MFA), further strengthens defenses against unauthorized remote access attempts. Together, these measures reinforce network and system security, making it more difficult for attackers to breach.

5. Logging and Monitoring:

- **Default Settings:**
  - Basic logging configurations may be enabled.
- **Recommended Settings:**
  - Configure advanced logging and regularly review audit logs for security events.
- **Security Implications:**

Comprehensive logging enables proactive detection of suspicious activities and facilitates rapid response to potential incidents.

6. Firewall Configuration (Windows Defender Firewall):

- **Default Settings:**
  - Default configuration allows incoming connections from the network list and blocks others.
  - Logging: The size limit is set to 4096 KB, Sometimes by default: logging keeping is avoided.
- **Recommended Settings:**
  - Define custom rules for traffic management, enable Intrusion Prevention System (IPS), and implement VPNs for network access control.
  - Ensure 'Windows Firewall Logging: Size limit is set to 16,384 KB or greater and keep loggings.
- **Security Implications:**

Defining custom traffic rules, enabling Intrusion Prevention Systems (IPS), and implementing VPNs ensure granular control over network access and enhance protection against threats. Setting the Windows Firewall log size to 16,384 KB or greater and maintaining logs improves visibility into network activities, aiding in monitoring and forensic analysis

7. Advanced Audit Policy Configuration :

- **Default Settings:**
  - Basic audit policies may vary depending on customization (As an example Audit Credential Validation is set to Success where it should be changed to Success and Failure).
- **Recommended Settings:**

- Create audit filters for key areas, audit both successful and failed attempts.
- Regular log review and archiving.

- **Security Implications:**

To improve security, implement targeted audit filters for key system activities such as logon and logoff events, focusing on both successful and failed attempts. Additionally, establish a regular log review process and ensure logs are archived securely to detect suspicious activities promptly and prevent unauthorized access.

8. Administrative Templates:

- **Default Settings:**
  - This covers a whole lot of areas with some default values.
  - Enhanced Security Configuration for Internet Explorer and real-time protection enabled.
- **Recommended Settings:**
  - Enable automatic updates, review security zone settings, and configure Real-time Protection.
- **Security Implications:**

Automatic updates ensure the timely application of security patches, reducing vulnerabilities. Real-time Protection safeguards the system by continuously monitoring and defending against malware.

Rocky Linux 9

1. Filesystem Configurations:

- **Default Settings:**
  - Default configurations may include standard filesystem permissions and unencrypted partitions.
  - By default, a single root (/) partition is used.
  - Default mount options for XFS include options like rw (read-write), relatime (relative access time), and noatime (no access time updates) on some partitions.
- **Recommended Settings:**
  - Configure separate encrypted partitions for sensitive directories like /var, /tmp, and /home.
  - Schedule regular filesystem checks using fsck to detect and repair potential filesystem issues.
  - Apply restrictive permissions to sensitive directories to limit access to authorized users only.
- **Security Implications:**

Configuring separate encrypted partitions for sensitive directories like /var, /tmp, and /home safeguards data by isolating and protecting it from unauthorized access. Regularly scheduling filesystem checks with fsck helps identify and fix potential issues, preventing exploitation of vulnerabilities. Applying restrictive permissions limits access to authorized users only, reducing the risk of unauthorized modifications and enhancing overall system security.

2. Service Settings:

- **Default Settings:**
  - Services are often running with default configurations and may include unnecessary services.
- **Recommended Settings:**
  - Disable non-essential services and adjust startup types as needed.
- **Security Implications:**

Reducing unnecessary services minimizes potential attack vectors by limiting exposure to vulnerabilities. It also enhances system performance by freeing up resources and reducing complexity.

3. User and Account Management:

- **Default Settings:**
    - By default, users may have broad permissions and generic account settings, which can lead to excessive access rights and potential security risks.
- **Recommended Settings:**
    - Implement robust access controls using SELinux to enforce fine-grained permissions.
    - Apply the principle of least privilege to ensure users have only the minimal access necessary for their tasks.
    - Regularly audit user accounts to identify and address any inappropriate access or outdated accounts.
- **Security Implications:**

Strong access controls with SELinux and least privilege principles significantly reduce the risk of unauthorized access and limit the potential damage from compromised accounts. Regular audits ensure that any anomalies or security gaps are promptly addressed, enhancing overall system security.

4. Logging and Monitoring:

- **Default Settings:**
    - Basic logging configurations may be enabled by default.
- **Recommended Settings:**
    - Enhance logging configurations to capture comprehensive details, including authentication events, file access, and administrative actions.
    - Implement a routine to regularly review logs for suspicious activity and potential security incidents.
- **Security Implications:**

Enhanced logging and consistent monitoring improve the ability to detect and respond to security incidents promptly. This proactive approach allows for the early identification of anomalies, aiding in the timely mitigation of threats and strengthening overall system security.

5. Firewall Configuration (Firewalld):

- **Default Settings:**
    - By default, Firewalld may come with pre-configured rules that allow certain types of traffic, which might not be optimized for security.
- **Recommended Settings:**
    - Configure rules to block all incoming traffic by default and allow only necessary connections.
- **Security Implications:**

Properly configuring Firewalld to block all incoming traffic by default minimizes the attack surface and protects against unauthorized access, enhancing overall system security. This approach ensures that only essential services are exposed, reducing the risk of potential exploits.

6. Advanced Security Policies:

- **Default Settings:**
    - Basic security policies may be in place.

- **Recommended Settings:**
    - Implement SELinux for enforcing access control policies, configure AppArmor for additional security layers, and ensure secure boot processes.
- **Security Implications:**

Advanced security policies harden the system against various attack vectors, making it more resistant to breaches and malware.

4. Proposal for Implementation for Future Server Installations

Based on the analysis, Pandora Company Limited should adopt the following structured approach to implement hardening measures for upcoming server installations:

- **Rocky Linux 9:**
    - Configure encrypted partitions, especially for sensitive directories like /var and /home.
    - Disable non-essential services to reduce the attack surface and improve performance.
    - Secure network interfaces by configuring firewalld and enforcing access controls with SELinux.
    - Enhance logging configurations using Systemd Journal and regularly monitor logs for anomalies.
    - Ensure consistent system updates and patches through automated tools like dnf-automatic to maintain security.
- **Windows Server 2019 R2:**
    - Strengthen account policies with strict password policies and lockout mechanisms.
    - Minimize running services by disabling unnecessary roles and features.
    - Customize Windows Defender Firewall rules to restrict inbound and outbound traffic to only essential services.
    - Implement advanced audit policies to log both successful and failed access attempts, enabling proactive threat detection.
    - Secure system settings via administrative templates for both computers and users, ensuring alignment with company security standards.

The implementation will be rolled out in a phased approach over several weeks. The process begins with preparation and inventory assessment, followed by applying the hardening measures on each server environment. This will be followed by continuous monitoring, regular security audits, and staff training to ensure consistent adherence to these measures and prompt detection of any vulnerabilities. Future server installations should adhere to these security baselines from the outset to maintain a secure infrastructure.

5. Summary

By implementing the CIS Benchmarks, Pandora Company Limited will greatly strengthen its cybersecurity posture. These measures address vulnerabilities arising from default system configurations, significantly reducing the company's exposure to potential threats. The recommended hardening practices not only minimize the attack surface but also enhance overall system stability and resilience. This proactive approach safeguards existing infrastructure while ensuring that future installations meet the highest security standards. Through consistent monitoring, regular security audits, and comprehensive staff training, Pandora Company Limited will be well-equipped to protect its critical assets and maintain robust cybersecurity defenses in an evolving threat landscape.

6. References

- CIS intro : Link
- CIS_Microsoft_Windows_Server_2019_Benchmark_v3.0.1
- Firewalld Documentation: Link
- Microsoft Security Baselines: Link
- Windows logging & monitoring : Link
- CIS_Rocky_Linux_9_Benchmark_v2.0.0
- Rocky Linux file systems : Link
- Rocky Linux service guide : Link
- Linux policies : Link