

Pandora network diagram and possible improvements – Week 1

Here is the current setup of Pandora Company:

Servers:

1. **Web Server:** Hosts <http://www.pandora.lk>. [note: will be enabled later] This is an Apache web server running on Rocky Linux 9 Server, assigned the static IP address 192.168.1.10.
2. **Application Server:** This server hosts internal web applications for Pandora employees, such as the Leave System and Order Management system. It operates on Windows Server 2019 R2 and is assigned the static IP address 192.168.1.15.
3. **Database Server:** This MySQL/MariaDB Server hosts databases for both the Web Server and Application Server. It runs on Rocky Linux 9 and has been assigned the static IP address 192.168.1.20.

Departments and Devices:

Pandora Company consists of the following departments, each with a certain number of PCs connected to the network via DHCP:

- Sales (4 PCs)
- Engineering (5 PCs)
- Production Equipment (10 PCs)
- HR (2 PCs)
- Legal (2 PCs)
- IT (2 PCs)


Additionally, the network also includes 4 CCTV IP cameras.

The company uses a fiber internet connection with a static public IP provided by the ISP. This static public IP is directed to the web server. All the servers, IP cameras, and PCs are on the 192.168.1.0/24 network and have internet access.

Your Task for This Week:

This week, your primary task is to draw a network diagram representing the current setup and to suggest potential network segmentation. In addition, please identify any additional devices that may be required for this segmentation and propose potential configurations or access control rules for those devices.

We're looking forward to seeing your ideas on improving the security posture of Pandora Company Limited. Good luck!





Week Two at Pandora Company Limited: A Disturbing Discovery

After a detailed initial assessment of the IT infrastructure at Pandora Company Limited, you've made a concerning discovery. All operating systems on the servers appear to be running on default installation settings and configurations. This is a highly risky practice and leaves the company vulnerable to a myriad of potential cyber threats.

The existing setup includes:

1. Web Server: Apache web server running on Rocky Linux 9 Server.
2. Application Server: Internal web applications on Windows Server 2019 R2.
3. Database Server: MySQL/MariaDB on Rocky Linux 9.

The lack of security hardening on these systems is a serious oversight. As the consulting security engineer, you must address this critical gap in Pandora's cybersecurity posture.

Assignment Tasks:

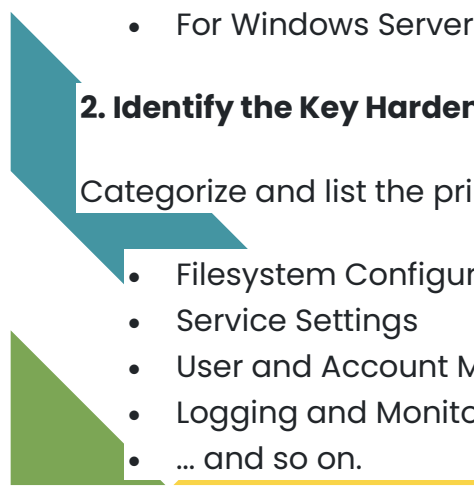
1. Identify a Reputed Hardening Framework:

Considering the operating systems in use, identify a trusted and globally recognized framework for security hardening. One suggestion is the Center for Internet Security (CIS) benchmarks. However, you may propose any other recognized standard, provided you justify its reliability and applicability.

- For Rocky Linux 9, find and retrieve the matching CIS benchmark (or from your chosen framework). If not directly available, leverage the closest version or a general guideline and adapt accordingly.
- For Windows Server 2019 R2, get the relevant hardening guideline.

2. Identify the Key Hardening Sections:

Categorize and list the primary sections these guidelines address. Examples include:

- Filesystem Configurations
 - Service Settings
 - User and Account Management
 - Logging and Monitoring
 - ... and so on.
- 



3. Analyze and Document Improvements over Default Settings:

For each of the identified key sections:

- a) **State the Default Settings:** Describe the initial configuration that typically comes with a standard OS installation.
- b) **State the Recommended Settings:** Highlight the hardening measures proposed by the chosen framework.
- c) **Discuss the Security Implications:** Detail how the recommended setting improves security over the default configuration, making the system more resilient against potential cyber threats.

4. Proposal for Implementation for Future Server Installations:

Based on your analysis, provide a clear and structured plan for Pandora Company Limited to implement these hardening measures in upcoming server installations.

Deliverables

Report Content:

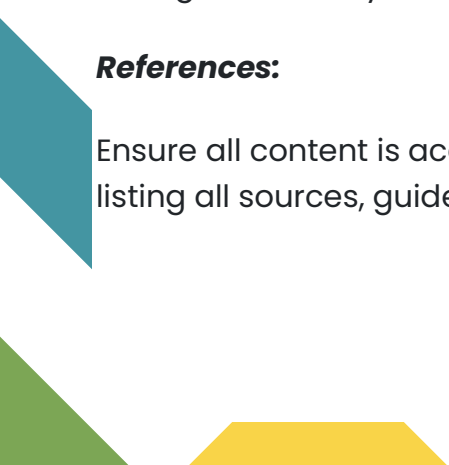
Produce a 3-4 page PDF report addressing the assignment tasks outlined earlier.

Detail the importance of OS security hardening, emphasizing the implications for Pandora Company Limited.

Summary:

Conclude with a succinct summary highlighting the overall significance of the proposed changes for the cybersecurity posture of Pandora Company Limited.

References:



Ensure all content is accurately cited. Include a references section at the end of your report, listing all sources, guidelines, and materials consulted during your analysis.

Project Part 3 – Week Four at Pandora Company Limited: Web Woes Uncovered

You've discovered that the corporate website, explicitly served over <http://www.pandora.lk>, was developed using WordPress and launched two years ago. After its inauguration, the website's developers provided the admin credentials in a sealed envelope and concluded their engagement. Remarkably, since its launch, the sealed envelope containing the admin credentials hasn't been opened by any member of the technical team.

The website hosts a "Sales Inquiries" form. This form gathers several pieces of data from potential clients, notably their Name, Mobile Number, Date of Birth, NIC, and Home Address.

A preliminary glance at certain configuration files indicates that the WordPress installation utilizes the MySQL/MariaDB root user for database interactions.

Assignment Tasks:

- Assess the Current State: Enumerate potential risks based on your observations and drawing from best practices in cybersecurity.
- Identify Potential Vulnerabilities: What could be the potential vulnerabilities or misconfigurations?
- Propose Security Interventions: Reflecting on your discoveries, recommend security measures that could bolster the website's security posture. It's vital to consider the broader ramifications of each vulnerability you identify.
- Recommend Best Practices for the Future: Beyond immediate issues, contemplate the website's continuous security and maintenance. How can Pandora Company Limited ensure the site stays secure and current?

Deliverables

Report Content:

Compose a 2-3 page PDF report addressing the assignment tasks described above.

References:

Ensure every piece of content is cited appropriately. Conclude your report with a references section, listing all sources, guidelines, and materials you've referred to during your analysis.

Week Six at Pandora Company Limited: Bridging the Islands of Systems Chaos

During your ongoing tenure at Pandora Company Limited, you've discovered that 25 individual Windows PCs operate across various departments. Each PC has its setup, resulting in a lack of uniformity concerning user policies, software installations, and security configurations. Observations include employees using unsafe passwords like "1234", challenges in deploying updates uniformly across all computers, and inconsistent access restrictions. You believe there's an opportunity to recommend a more centralized user/system management approach, addressing many observed challenges.

Assignment Task:

Unified Management Exploration:

- What are the cybersecurity challenges and risks a company faces with a decentralized PC management system?
- Propose a commonly-adopted enterprise solution to address the issues observed at Pandora Company.

Advantages & Benefits Analysis:

- Dive into the benefits of transitioning to a unified user/system management system.
- Additionally, reflect on potential indirect advantages.

Recommendation Report:

- Based on your exploration and analysis, prepare a detailed recommendation for Pandora Company Limited.
- Outline the steps the company should take to transition from its current decentralized approach to a centralized system. This should encompass both technical actions and potential change management strategies.

Deliverables:

Report Content: Craft a comprehensive 3-4 page PDF report addressing the assignment tasks. Clearly segment your report into sections: Unified Management Exploration, Advantages & Benefits Analysis, and Recommendation Report.

References: Ensure all content is properly cited. At the conclusion of your report, list all sources, guidelines, and materials referenced during your analysis.