Securing a Financial Institution’s IT Infrastructure

Scenario:  
**You have been hired as a cybersecurity consultant** for FinSecure Bank, a mid-sized financial institution that has recently experienced a cyberattack. After an initial investigation, it was revealed that the breach occurred due to a combination of system administration errors, misconfigurations, and lack of proper security controls. **Your task is to analyze the security issues, assess the potential impact, and propose mitigation strategies to secure the bank’s infrastructur**e.

Assignment Tasks:

1. Identify Security Issues  
   Based on the investigation report, the following security weaknesses were found:
   * Default configurations were left unchanged on several internal servers.
   * Logging and monitoring were either disabled or inadequately configured.
   * Some systems were running outdated software versions.

Task:

* + Analyze each security issue and explain how it could have contributed to the breach.
  + Provide at least two real-world examples or case studies for each type of issue.

1. Impact of Misconfigurations  
   Further assessment highlighted these critical misconfigurations:
   * Firewall rules allowed unrestricted inbound traffic from untrusted networks.
   * APIs used for mobile banking were unsecured, exposing sensitive customer data.
   * Hardcoded credentials were found in publicly accessible source code repositories.

Task:

* + Describe the possible consequences of each misconfiguration.
  + Discuss how these misconfigurations can be exploited by attackers, using practical examples.

1. Mitigation Techniques  
   The bank’s leadership has asked you to propose a set of mitigation techniques to strengthen their security posture.

Task:

* + Recommend solutions based on the following areas:
    - Implementing least privilege access control.
    - Performing regular system audits and hardening.
    - Conducting security training for system administrators.
  + For each recommendation, provide an implementation plan with specific steps.

1. Conclusion and Action Plan  
   Summarize your findings and create a 3-month action plan to address these security issues and prevent future incidents. The action plan should include short-term, mid-term, and long-term steps. Suggest a security check list for the administrators