Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. **Port Filtering** 2. **Encryption** 3. **Firewall Configuration**

Part 2: Explain your recommendations
1. **Port Filtering** Port filtering controls which communication ports are allowed or blocked on a network. By only keeping necessary ports open (like 443 for HTTPS) and blocking unused or risky ones, we reduce the number of entry points an attacker could exploit. This minimizes the attack surface and prevents unauthorized services from running undetected. This setting should be reviewed and updated whenever new applications are introduced or at least once per quarter. 2. **Encryption** Encryption protects sensitive data by converting it into an unreadable format unless a person has the right decryption key. If attackers gain access to stored information or intercept network traffic, encryption ensures the data remains protected. It's especially useful for safeguarding personal information, passwords, and communication between systems. Encryption should be continuously enforced, and the protocols and keys should be audited regularly—such as annually or during any system changes.

3. **Firewall Configuration**
   A firewall acts as a gatekeeper for network traffic. Without proper rules, anything can come in or out. By setting rules that control traffic based on IP addresses, protocols, or ports, we can block harmful data and only allow trusted sources. This helps protect internal systems from external threats and reduces the risk of malware or data leaks. Firewall rules should be reviewed after any major network updates and at least quarterly to stay aligned with evolving security needs.