# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Patch Updates 2. Port Filtering 3. Firewall Maintenance 4. Network log Analysis |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. Port filtering: it blocks and allows certain port numbers on the firewall to limit unwanted communication. It is used to control network traffic and can prevent potential attackers from entering the private network. 2. Patch Updates: A software or Operating system update that addresses within a program or product. They often contain fixes to the security problems. It is important to keep the systems updated since with latest patches since the attackers will be alerted to the security vulnerability when patches are released. They will target the vulnerability before people eventually apply those patches. 3. Firewall maintenance: Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. 4. Network log: The process of examining network logs to identify events of interest. Can be configured to alert the security team when there is abnormal traffic on the network. This can be used either before an incident occurs, during to track network traffic, and can be configured in the response of a cybersecurity attack. A common tool used for analyzing network logs is a SIEM. |
|  |
|  |