Prevention

- Ensure that all software is up to date to patch the bug in the service.
- Standardize the software and ensure that users cannot install software onto the system without approval to prevent anyone from installing a malicious software inside the system
- Do not allow anonymous login for services such as FTP and SMB
- Install a firewall to block traffic that are malicious in nature
- Remove any services that are no longer in use
- Close any ports that are no longer in use
- Remove users and data linking to the users that do not exist
- Ensure services are not run as root
- Ensure that the permission value is set appropriately especially for files that contains sensitive information such as the password folder
- Set up proper access control to allow only certain groups of people can access the system
- Use IDS/IPS to track potential packet flood
- Use network segmentation
- Use a strong password when creating an account
    - Setting a strong password means:
        - password is not the default password
        - password used is not notoriously weak
        - password that is a common phrase or word
        - passwords that does not include your birthday.

    - Other aspect to avoid
        - use of password hints
        - adding the season or month or year at the end or front of the website name.
        - using the same password for more than one account
        - sharing of password with others