Hardening Against Open SSh on Target 1

There are a wide variety of hardening techniques for SSH. These can include:

- Set a custom TCP port by editing the */etc/ssh/sshd_config* file.
- Filter the SSH port through the firewall
- Implement SSH Passwordless Login. Uses keys to allow for login and removes the password prompt
- Disable empty passwords
- Set a custom SSH login banner. Doesn’t stop logins but is a warning of active monitoring
- Keep SSH updated