# TTP Detail – T1142

## TTP Information

Name: Keychain

Description: Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and Kerberos. Keychain files are located in <code>~/Library/Keychains/</code>,<code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>. (Citation: Wikipedia keychain) The <code>security</code> command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

To manage their credentials, users have to use additional credentials to access their keychain. If an adversary knows the credentials for the login keychain, then they can get access to all the other credentials stored in this vault. (Citation: External to DA, the OS X Way) By default, the passphrase for the keychain is the user’s logon credentials.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access