Beyond the good ol' LaunchAgents - 6 - SSHRC

theevilbit.github.io/beyond/beyond_0006

March 21, 2021

> This is part 6 in the series of "Beyond the good ol' LaunchAgents", where I try to collect various persistence techniques for macOS. For more background check the introduction.

I learned about this trick from @0xdade when he posted it on Twitter.

If we create a file in the user's HOME directory at `~/.ssh/rc` it will be executed prior to the user's login shell becomes available. The man page of `sshd` describes this in more detail.

```
 If ~/.ssh/rc exists and the sshd_config(5) PermitUserRC option is set, runs it; else
if /etc/ssh/sshrc exists, runs it; otherwise runs xauth.  The ``rc'' files are given
the X11 authenti-cation protocol and cookie in standard input.  See SSHRC, below.
```

and some more.

```
SSHRC
     If the file ~/.ssh/rc exists, sh(1) runs it after reading the environment files
but before starting the user's shell or command.  It must not produce any output on
stdout; stderr must be used
     instead.  If X11 forwarding is in use, it will receive the "proto cookie" pair
in its standard input (and DISPLAY in its environment).  The script must call
xauth(1) because sshd will not run xauth
     automatically to add X11 cookies.

     The primary purpose of this file is to run any initialization routines which may
be needed before the user's home directory becomes accessible; AFS is a particular
example of such an environment.

     This file will probably contain some initialization code followed by something
similar to:

        if read proto cookie && [ -n "$DISPLAY" ]; then
                if [ `echo $DISPLAY | cut -c1-10` = 'localhost:' ]; then
                        # X11UseLocalhost=yes
                        echo add unix:`echo $DISPLAY |
                            cut -c11-` $proto $cookie
                else
                        # X11UseLocalhost=no
                        echo add $DISPLAY $proto $cookie
                fi | xauth -q -
        fi

     If this file does not exist, /etc/ssh/sshrc is run, and if that does not exist
either, xauth is used to add the cookie.
```

If we have root access we can also create `/etc/ssh/sshrc`.

We can disable it by setting `PermitUserRC no` in `/etc/ssh/sshd_config`.