PAM

Pluggable Authentication Modules (PAM)

PAM is essentially an authentication system that allows for different modules to be added for support of different authentication methods, as an example; 2fa would be handled by PAM on a Linux system.

/etc/security/

==========

Lockout Policies

FailLock

FailLock is a PAM module used for tracking failed authentication attempts in Linux systems.

It is primarily used to prevent brute force attacks by locking out user accounts after a specified number of consecutive failed login attempts.

Key Features of faillock

- Account Lockout: Locks a user account after a specified number of failed authentication attempts.
- Unlocking: Automatically unlocks the account after a specified period, or an administrator can manually unlock it.
- Logging: Records failed login attempts and lockout events, which can be useful for security auditing.

Pam_Tally2

Pam_Tally2 is the older version of failock which essentially does the same thing, just with fewer features. You'll potentially need to use this on older servers as they may not support failock.

Pam_Tally2 configuration file - /etc/pam.d/login

The below example locks users out after 3 failed logins, denies any root login attempts, and keeps accounts locked for 1 hour.

```
#
# The PAM configuration file for the Shadow `login' service
#

auth required pam_tally2.so deny=3 even_deny_root unlock_time=3600
```

==========

2-Factor Authentication (2FA)

2FA can be configured for SSH logins to servers. You'll most likely want to configure 2FA using PAM modules.

Cisco DUO

https://duo.com/docs/loginduohttps://duo.com/docs/loginduo#:~:text=Duo%20configuration.-,Install%20from%20Linux%20Packages,-To%20more%20easily

1. Create an account for Duo here

2. Add an 'application' to protect with duo
   application type in this case will be 'UNIX application'
   Once created, you'll be given access to the keys required for setting up DUO

3. DUO configuration on server:

   Ubuntu 22 example

add repo key and install duo

Create /etc/apt/sources.list.d/duosecurity.list with the following contents:

```
deb [arch=amd64] https://pkg.duosecurity.com/Ubuntu jammy main
```

```
curl -s https://duo.com/DUO-GPG-PUBLIC-KEY.asc | sudo gpg --dearmor -o
/etc/apt/trusted.gpg.d/duo.gpg
```

```
apt-get update && apt-get install duo-unix
```

Once installed, you can configure duo from /etc/duo

in `/etc/duo` add the integration key, secret key, and API hostname from your Duo Unix application.

As a regular user, test `login_duo` manually by running

```
/usr/sbin/login_duo
```

You'll be given a link at this point which can be used to configure your 2FA device.

Once you've tested that this is working, we can then look to implement duo to the SSHD and PAM config.

Edit /etc/pam.d/sshd and add the below:

```
auth requisite pam_unix.so
auth [success=1 default=ignore] /lib64/security/pam_duo.so
auth requisite pam_deny.so
```

Note: On some systems, the path to `pam_duo.so` might be `/lib/security/pam_duo.so`.

Edit the /etc/ssh/sshd_config and add:

```
UsePAM yes
ChallengeResponseAuthentication yes
```

Restart the SSHD service and test the configuration.

Revision #8
Created 2024-05-26 19:12:21 UTC by Daniel
Updated 2024-06-21 17:21:35 UTC by Daniel