GreenRocket
Security

ENABLE TWO-FACTOR AUTHENTICATION FOR DESKTOP LOGIN ON MACS USING GREENRADIUS

INTRODUCTION

This document helps you to set up two-factor authentication for desktop login on Macs using our GreenRADIUS server.

PREREQUISITES

Mac / macOS High Sierra (10.13.2).

STEPS:

1. Ensure 'System Integrity Protection' is disabled on your Mac. To disable it, follow the steps below:

    i. Boot your machine in recovery OS mode (restart your machine and hold down command and R keys).

    ii. From the terminal, run the following command:

    ```
    $ csrutil disable
    ```

    iii. Restart the Mac

2. Log on to the Mac using Administrative (super user) privileges, and copy this PAM module (`pam_radius_auth.so.2,` [linked here]) to the folder `/usr/lib/pam`

3. Create a configuration file named *`server`* in the folder `/etc/raddb`

In the file `/etc/raddb/server`, enter the details of the RADIUS server in the following format:

```
<IP address of GreenRADIUS> <shared secret> <timeout in seconds>
```

For example:

```
10.61.0.101 test 30
```

4. Add the following line at the top of the file `/etc/pam.d/authorization`

```
    auth     sufficient        pam_radius_auth.so
```

5. Add the IP address of the Mac as a RADIUS client in GreenRADIUS
    I. Log in to GreenRADIUS from its web administration console and navigate to Domain-> <domain name > ->RADIUS Clients -> ‘Add Client’
    II. Fill the details of the Mac in the "Add Client" section:
        - For example, if your Macbook’s IP address is "10.51.0.50" and the shared secret is “test” (same as the one configured in step 3 above in the /etc/raddb/server file on the Mac)
            - set "Client IP": 10.51.0.50
            - set "Client Secret": test
            - set "Confirm Client Secret": test
6. Restart the Mac and test the authentication using GreenRADIUS.

Enable Second Factor Authentication for SSH access to the MacBook

Add the following line at the top of the file /etc/pam.d/sshd

```
auth     sufficient       pam_radius_auth.so
```

✦✦✦