Introduction

Why

After the recent increase in hacker activity and floods of phishing emails, it is clear that the Observatory Compute environment is under constant attack. One of the major deficiencies in our current setup is that it is enough to know a username and password to get access to a wide variety of resources and data. With the improper handling of phishing emails, but also when using public wifi services, it seems easy for people with not so good intentions to get account credential information. After that, there is no easy way to prevent misuse of accounts and computer resources.

We need to put a stop to that, and the only way to do that is to introduce a second step in identifying that you are the rightful owner of the account credentials. This second step is provided throught the Two-Factor Authentication (2FA) mechanism. For this second verification, you need a physical device, for instance a smart phone or personal computer.

Where

In principle for every service where you need to identify yourself, 2FA is needed. In the beginning we will restrict 2FA to two major services: Web pages and ssh remote login. At a later stage 2FA will be implemented for other services as well. You will be informed well in advance.

WEB Pages & 2FA

For all Web pages where you need to login, we will enforce 2FA. This also, and in particular, includes webmail. The Observatory WEBsite has many pages shielded by authentication and each page will be individually added to the 2FA facility.

ssh remote login & 2FA

One other major way to gain access to our resources and data is through the ssh protocol. So this means that using `ssh` to login from remote to the Observatory ssh gateway or to the local desktops or servers, you will be confronted with a second prompt to enter credentials. How this works is explained later on this page. In fact, 2FA is imposed on the ssh protocol, so `scp`, `sftp`, remote `rsync` and even tunnelier (Win) will also be affected.

How

The 2FA protocol that we have implemented is based on the Time-based One Time Password (TOTP) mechanism and we are using RedHat developed tools to implement this. TOTP means that for a limited amount of time you get a passcode, which you have to provide to the authentication program as a second 'password' to gain access to the resource. Initially, at first use of 2FA, you have been given a private secret key and have stored that on your mobile device. Then, for each login, you use that mobile device to generate (time limited) passcodes. This passcode you present (type in) to the

login procedure and after verification it gives you access to the restricted resource. Details on this process are described below.

From:
https://helpdesk.physics.leidenuniv.nl/wiki/ - **Computer Documentation Wiki**

Permanent link:
https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=lion:2fa:introduction&rev=1616442127

Last update: **2021/03/22 19:42**