Linux Authentication 1FA Passwordless or 2FA – How does it work?

AuthNull

Table of Contents

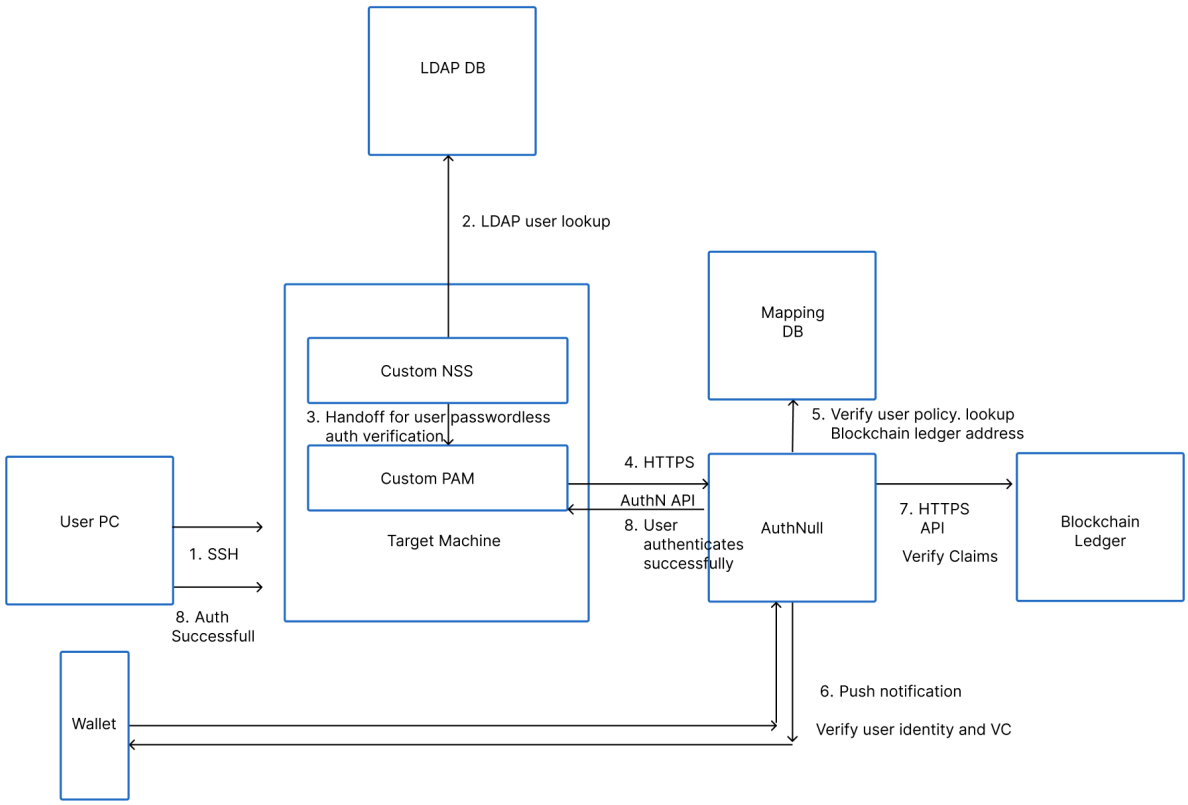
Overview

This document provides an overview of AuthNull's 1FA passwordless authentication design for Linux systems.

The same can be delivered as 2FA together with SSHD / SSSD against Active directory. This solution assumes that these machine credentials are validated against an active directory and therefore uses SSSD (for 2FA) or Custom NSS for 1FA authentication.

Use case #1: Interactive Passwordless authentication

Logical architecture and flow



Steps	What happens
Step #1	User attempts to connect to target machine using SSH Ssh asif@1.1.1.1
Step #2	Custom NSS module does a directory lookup to verify the user identity on an LDAP directory (LDAP / TCP). When successful this moves to step #3. If not successful – authentication will be denied. In cases of using SSSD – SSSD does a full password / SSH Key validation (together with SSHD) providing a 2FA authentication design.

Step #3	Custom PAM module initiates Passwordless authentication from wallet
Step #4	SSP server gets called to verify interactive authentication policy from the mapping db.
Step #5	Mapping DB is used to look up authentication policy and verify - Does this user actually have access rights? Does an interactive policy exist? - Lookup Address of blockchain ledger.
Step #6	User / Owner of account gets a push notification on wallet - User submits presentation submission (credential signed by private key) if he accepts the authentication request, or deny the request if they think someone else is accessing the account. - This PR can be verified using users public key - Additionally, it is converted to a hash with current salt and random string for the day. - This can be considered as user Hash
Step #6	The blockchain ledger hash is looked up from the address from Mapping DB for this user authentication policy. This hash is compared to the computed hash retrieved from the wallet. If both the hashes match, it further verifies that the user has the correct credentials using blockchain
Step #7	User is able to authenticate successfully.