Harden users’ passwords by rejecting the ones that contain a username

Task 1. Do not use your username in password

1. Create and run a script (Ansible playbook) to harden users’ passwords by rejecting the ones that contain a username. Enforce this rule for ‘root’ as well.
2. [Optional] Try to implement the same hardening rule without PAM

(pluggable authentication module).

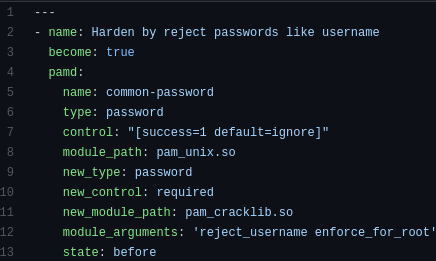
1. Write a report in Google Doc providing the playbook’s code and proof of workability (screenshots or asciicinema recording)

Target platform: any Linux-based distribution

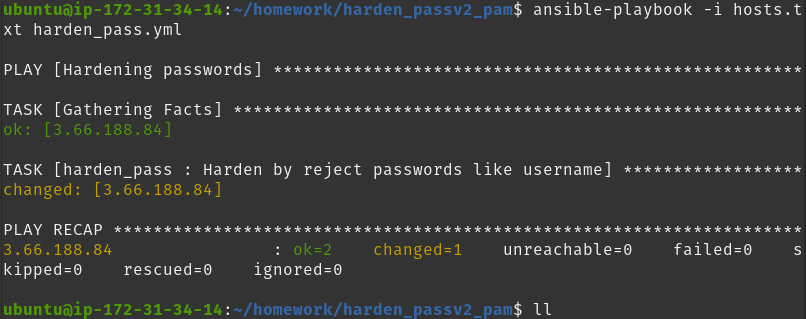
Solution:

To ensure user password will not contain username we can use pamd module ansible or use shell module as second option to edit configuration files in /etc/pam.d directory.

1. The first way is to use the pamd module. I used roles to get reusable code.

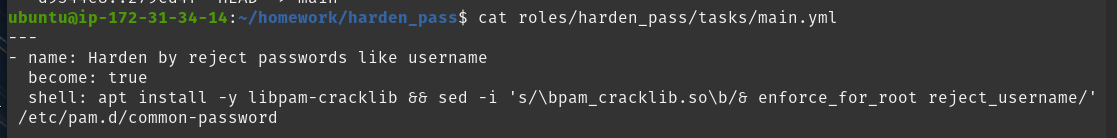


The code of role using pamd module

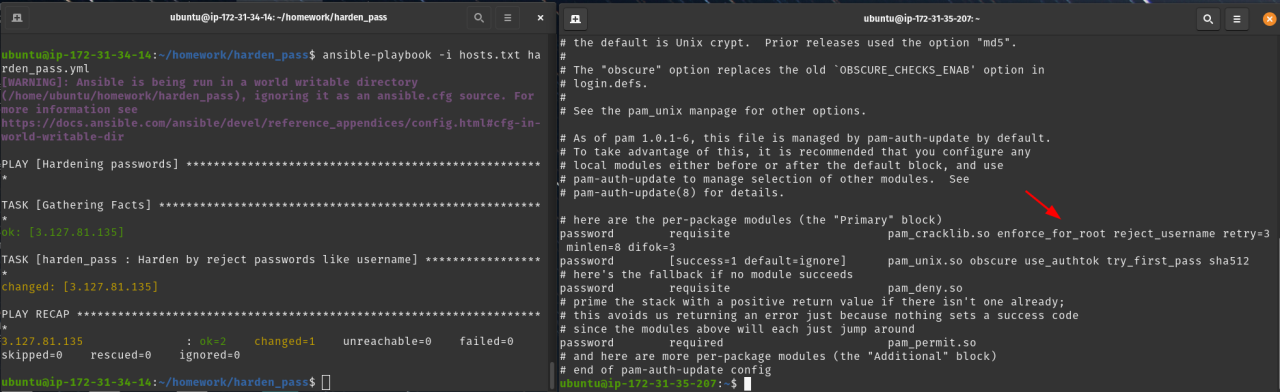


The result after running the playbook with pamd module

1. [Optional task] The second to perform ansible is to use shell module and bash commands. Using this way we need to edit file /etc/pam.d/common-password and add there pam\_cracklib module with needed arguments.

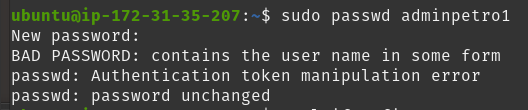


Code of the ansible role for this

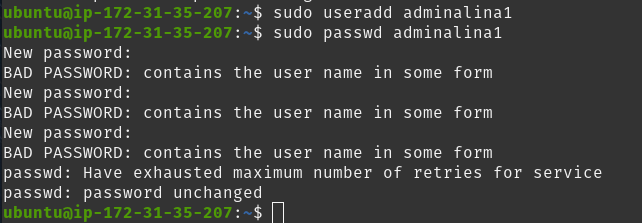


Result of executing playbook with shell module

Testing result by adding new user and creating the password the same as username for the new user:



The result of tests after using the 1-st way with pamd module



The result of tests after using the 2-nd way with shell module

The full code you can find in the github repository: <https://github.com/andrikstravinsky/GLBaseCamp2021>