Hardening Homework

[DevOps BaseCamp 2021]

Author: **Oleksandr Bokotei**

GitHub repository:

https://github.com/nonamecoder2002/GLBaseCamp2021/tree/main/Hardening_Homework

Task 1: “Do not use your username in password”

The code below hardens users’ & root`s passwords by rejecting the ones that contain their login:

```
---
- hosts: all
  remote_user: root
  tasks:
    - name: Installing pwquality module
      apt:
        name: libpam-pwquality
        update_cache: yes

    - name: Configuring pwquality module
      pamd:
        name: common-password
        type: password
        control: requisite
        module_path: pam_pwquality.so
        module_arguments: 'usercheck=1 enforce_for_root retry=3'
        state: updated
```

To check out whether the code worked let's try to change password of root from `'1234'` to `'root1234'`:

```
root@remote-noodle:/etc/security# passwd
New password:
BAD PASSWORD: The password contains the user name in some form
New password:
```

As we can see, the code really works, so your login cannot contain your login

Task1 [Optional]: “Harden the passwords but without using pamd Ansible module”:

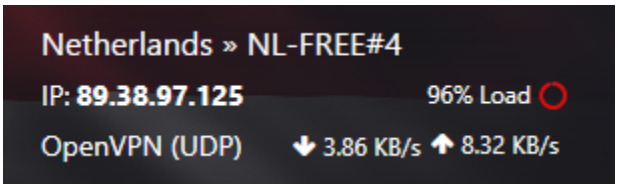
```
---
- hosts: all
  remote_user: root
  tasks:
    - name: Installing pwquality module
      apt:
        name: libpam-pwquality
        update_cache: yes

    - name: Configuring pwquality module
      lineinfile:
        path: /etc/security/pwquality.conf
        regexp: "{{ item.pattern }}"
        line: "{{ item.data }}"
        state: present
      loop:
        - {pattern: 'usercheck', data: 'usercheck=1' }
        - {pattern: 'enforce_for_root', data: 'enforce_for_root' }
        - {pattern: 'retry', data: 'retry=3'
```

Task 2: “Configure TCP Wrappers”

The code below hardens the sshd:

```
---
- hosts: all
  remote_user: root
  tasks:
    - name: Hardening the sshd
      lineinfile:
        path: /etc/hosts.deny
        line: "sshd: ALL EXCEPT LOCAL, {{ ansible_env['SSH_CLIENT'].split()[0] }}"
```

To check if the code works, let's turn on VPN and try to ‘ssh’ to our server:



VPN is turned on so we have new IP address

```
alex@DESKTOP-LBU2UOH:~$ ssh root@64.227.122.230
kex_exchange_identification: Connection closed by remote host
```

Indeed, we can't connect to the server from any IP except the ones that are specified in the code.