Minions Ubuntu 20 README

Please read the entire README thoroughly before modifying anything on this computer.

Forensic Questions

There are "Forensic Questions" on your Desktop; you will recieve points for answering these questions correctly. Valid (scored) "Forensic Questions" will only be located directly on your Desktop. Please read all "Forensic Questions" thoroughly before modifying this computer, as you may change something that prevents you from answering the question correctly.

Competition Scenario

Hello! The minions were trying to set up a new computer for Gru as a birthday gift, but we've struggled with securing our system! Additionally, some villains were able to sneak their way into our base! We need your help to secure the system, and its up to you to save us. Please take care of our security maintenance as well as other issues you find along the way.

Other minions have agreed that our security policies must require all minion accounts be password protected. Minions are required to choose secure passwords; however, this policy may not be currently enforced on this computer. It is very important to **write down all passwords you change**. The presence of any non-work related media files and "hacking tools" is strictly prohibited. We currently do not use any centralized maintenance or polling tools to manage our IT equipment. This system is for minion use only by authorized minions.

Additionally, Gru's wife, Lucy Wilde, would like to participate in this project, so please add her to the system as (lucywilde).

Ubuntu 20.04

We have also decided to use only Ubuntu 20.04 on this system. It is also a minion policy to use only the latest, official, stable Ubuntu 20.04 packages available for required software and services on this computer. Kevin has decided that the default web browser for all users on this computer should be the latest stable version of Firefox. The other minions have also decided on a policy to never let users log in as root. If administrators need to run commands as root, they are required to use the "sudo" command.

Authorized minions must be able to access this system remotely to communicate by using ssh.

Note: As this is a practice image, updates are **NOT** required, but configurations might be.

Critical Services:

- OpenSSH Server (sshd)

Authorized Administrators and Users

Authorized Administrators:
gru (you)
password: password
kevin
password: papaya
drnefario
password: b0og1eb%ts
lucywilde
password:

Authorized Users (Minions):
jerry
bob
phil

```
stuart
dave
carl
lance
donnie
john
mark
mel
```

Competition Guidelines

- In order to provide a better competition experience, you are **NOT** required to change the password of the primary, auto-login, user account. Changing the password of a user that is set to automatically log in may lock you out of your computer.
- Authorized administrator passwords were correct the last time you did a password audit, but are not guaranteed to be currently accurate.
- Do not stop the engine service. If stopped, enable the service again with **systemctl enable engine** and restart your VM.
- Do not remove any files from /opt/temp.
- Do not remove any authorized users or their home directories.
- The time zone of this image is set to PDT. Please do not change the time zone, date, or time on this image.
- This image was created for the sole purpose of training cyber students at Troy High School. This image should not be redistributed outside of Troy High School unless given proper authorization to do so.

Created by Derek Peng in collaboration with Benjamin Sheeh, Evelyn Cho, Gabriel Fok, Coco Gong, Johnny Ni, and Aaron Shan.