Warm Up: Submit a complex password (one you would use)

Introduction to Linux Security

WHEN YOU TELL EVERYONE TO USE TERMINAL FOR EVERYTHING BUT THEN USE GUI FOR CONFIGURING UPDATES

Update Configurations

- You can set the update configurations on the linux system through the GUI
- These configurations are used to make sure that the system updates and upgrades correctly
- Go to the update manager
- For the updates tab
  - Check for updates daily
  - Display Security Updates
    - Immediately
    - Weekly
    - for long term support versions
- For the Ubuntu Software Tab
  - Check downloadable from internet all checked
  - Download from server from United States (Make sure this is correct **)
  - Uncheck installable from CDROM
- For the Other Software Tab
  - The Canonical boxes are the only ones that are supposed to be checked

Updating

- Make sure you fix the update configurations before you do the actual updating
- There are two ways to update the linux system
- Command Line
  - sudo apt update && sudo apt upgrade -y
  - The update command gets a list of packages that need to be updated on the system
  - The upgrade command actually applies the updates to the entire system

REMEMBER:
nano to open files
cd to go to directories

DO NOT USE cd ON FILES

or that will be a certified bruh moment

Account Types

- Three types of users:
  - Standard: users that have basic access to the system
  - Administrators: users with some privileges allocated to them, such as adding users or access to certain files
  - Root User: user with all privileges
- You can manage these privileges in the sudoers file
  - sudoers file is a file Linux and Unix administrators use to allocate system rights to system users
  - It allows you to control what each kind of user can do
  - You can open the file /etc/sudoers with the command visudo

Configuration for the Sudoers file

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo         ALL=(ALL:ALL) ALL
```

Guest Account

- Some versions of linux come with a guest account that does not require a password to log in
- A guest user can access internet but cannot change settings
- You should disable the guest account
- Edit the files
  - Ubuntu 14: /etc/lightdm/lightdm.conf
  - Ubuntu 16: /usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf
- Add the line allow-guest=false at the end of the files
- Also make sure that any instances of autologin is not there in both files

The Group File

- Every user on the system is a part of a group
- Every user is also a group
- System Administrators are part of the sudo group,
  - Remember from the previous presentation that those users that can use sudo have root privileges
- Make sure that the administrators are in the correct group and that all other users are also in the correct groups by editing the /etc/group file
- Each group has its own group number
- To add a user to a group, go to the group name, add the name of the user after a comma before other users in that group
- To delete a user from a group take their name out of the line in the file for that group

The passwd file

- The /etc/passwd file is a text file that contains the attributes of (i.e., basic information about) each user or account on a computer running Linux
- Each line in /etc/passwd represents a single user
- Another way to delete a user, you delete the line
- Every user with the userid less than 1000 is a hidden user
  - A hidden user can be a system user
  - It can also be an unauthorized user that is not supposed to be on the system
- Users with user ids greater than 1000 are visible users

The shadow file

- The /etc/shadow file stores actual passwords in encrypted format for user accounts
- This is the hash of the password for user account and stores the encrypted version of the password and additional properties of the user password
- Basically, it stores secure user account information.
- All fields are separated by a colon (:) symbol.
- It contains one entry per line for each user listed in /etc/passwd file.

Password Aging Requirements

- Password aging is a mechanism that allows the system to enforce a certain lifetime for passwords.
- This ensures that passwords are changed occasionally, which is a good security practice.
- Most Linux distributions do not enable password aging by default, but it's very easy to enable
- First install libpam-cracklib
- Edit the /etc/login.defs file

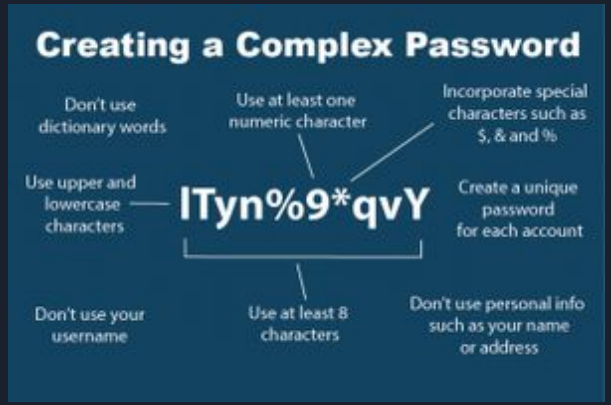
```
PASS_MAX_DAYS   15

PASS_MIN_DAYS   7

PASS_WARN_AGE   7
```

Password Complexity

- The more complex your password is, the harder it is to brute force and hack
  - Password complexity means making sure your password is harder to guess and predict, which can mean adding uppercase letters and lowercase letters, numbers, and symbols
- You can use PAM (the "pluggable authentication module") to enforce password complexity
- Edit the /etc/pam.d/common-password file

password requisite pam_cracklib.so try_first_pass retry=3 minlength=12 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 difok=4

sudo apt-get install libpam-cracklib



What do these parameters mean?

- try_first_pass = sets the number of times users can attempt setting a good password before the passwd command aborts
- minlen = establishes a measure of complexity related to the password length (more in a moment on this)
- lcredit = sets the minimum number of required lowercase letters
- ucredit = sets the minimum number of required uppercase letters
- dcredit = sets the minimum number of required digits
- ocredit = sets the minimum number of required other characters
- difok = sets the number of characters that must be different from those in the previous password

Pam Security Continued

- Edit the /etc/pam.d/common-password file

password [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512 remember=5

- This makes sure that users cannot use the last five passwords

common-auth

auth [success=1 default=ignore] pam_unix.so nullok_secure

auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900

Kahoot!

Click on the link below to access the kahoot:

https://play.kahoot.it/v2/?quizId=b859c427-3a8e-4c5a-b839-0e252d6ea4a4