Berlys Deardorff

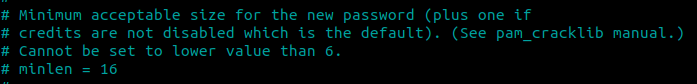
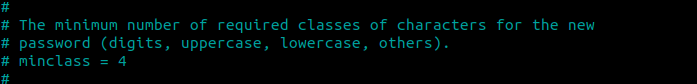
Homework 4

Linux-SysAdmin-Fundamentals

May 17, 2020

##Before you start scrolling, I didn’t decide to take screenshots until halfway through the assignment. Some of the earlier instructions don’t have screen shots because I couldn’t scoll back up to find them… sorry!

#Set Permissions on Sensitive Files:  
 read and write access  
read and write access  
 root read and write, everyone else read  
 root read and write, everyone else read   
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
#Create user accounts:  
sam, joe, amy, sara, admin  
- sudo adduser sam  
- sudo adduser joe  
- sudo adduser amy  
- sudo adduser sara  
- sudo adduser admin  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
#nano /etc/security/pwquality.conf  
  GNU nano 2.9.3              /etc/security/pwquality.conf              Modified  

  
  
  
  
#Force passwords to expire every 90 days:  
A picture containing orange, sitting, black, red

Description automatically generated  
    #Ensure that only admin had general sudo access:  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
#Create user group:  
  
    #add engineers group to system:  
- sudo addgroup engineers  
    #add users to managed group:  
A picture containing photo, black, red, computer

Description automatically generated  
    #create a shared folder /home/engineers  
- sudo mkdir /home/engineers  
    #change group on engineers directory to engineers group  
- sudo chown :engineers /home/engineers  
    #add GUID bit and stick bit to allow collab btwn engineers in this directory  
- sudo chmod 3777 /home/engineers  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

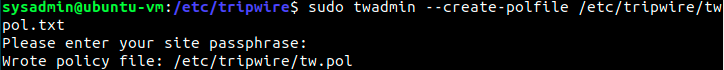
#Install and configure tripwire  
    #install tripwire:  
- sudo apt remove tripwire (removes older version; if installed)  
- sudo apt update (updates VM)  
- sudo apt upgrade (upgrades VM)  
- sudo apt install tripwire   
#Configure tripwire:  
- moved into /etc/tripwire directory to confirm you that twpol.txt  


#Comment out /dev and /proc files

A screen shot of a person

Description automatically generated

#Tell Tripwire to use recreated policy file:



#ran sudo tripwire --init

A picture containing orange, sitting, dark, black

Description automatically generated

#ran command:

* Sudo tripwire --check | grep -A 3 ^[1-9] > ~/research/tripwire.txt

#open ~/research/tripwire.txt

A screenshot of a cell phone

Description automatically generated

#ran command: sudo nano /etc/tripwire/twpol.txt

#commented out rulename =”Boot Scripts” file /etc/rc.boot/

A screenshot of a cell phone

Description automatically generated

#commented out rulename = “Root config files” left /root /root/.bashrc and /root/.bash\_history uncommented:

A picture containing sitting, table

Description automatically generated

#ran command to tell Tripwire to use recreated policy file:

A close up of a screen

Description automatically generated

#ran command to create database:

A screen shot of a computer

Description automatically generated

#ran command to run a system scan:



A screenshot of a cell phone

Description automatically generatedA screenshot of a cell phone

Description automatically generated

###Bonus###

#Ensure tripwire account doesn’t have a home folder:

A picture containing bottle, black, photo, orange

Description automatically generated

#Ensure tripwire account does not have a login shell:

* UID is under 1,000





#Ensure tripwire account is locked:

A picture containing sitting, black, table

Description automatically generated

#Ensure that tripwire account has UID < 1000

A screenshot of a cell phone

Description automatically generated

#Ensure that tripwire does not have a login shell:

A picture containing photo, sitting, black, table

Description automatically generated

#Ensure that tripwire can run the tripwire program using sudo:

* Ran command: sudo visudo
* Added tripwire ALL= NOPASSWD: /usr/bin/tripwire to file

A picture containing orange, dark, clock, food

Description automatically generated

#Install and run lynis:

* Install lynis

A picture containing photo, black, sitting, monitor

Description automatically generated

* Run audit

A screenshot of a cell phone

Description automatically generated

###BONUS###

#Install and run chkrootkit to verify system does not have root kit installed

A screenshot of a cell phone

Description automatically generated

* Ran command: sudo chkrootkit -x

A close up of a screen

Description automatically generated