Linux Fundamentals:

Link to challenge:

https://academy.hackthebox.com/module/18/section/94

(log in required)

Class: Tier 0 | Fundamental| General

Workflow:

System Information:

Question: Find out the machine hardware name and submit it as the answer

Answer: x86_64

Command: uname -i

Question: What is the path to the htb-student's mail?

Answer: /var/mail/htb-student

Command: env | grep mail

Question: Which shell is specified for the htb-student user?

Answer: /bin/bash

Command: cat /etc/passwd | grep htb-student | awk -F":" '{print $NF}'

Question: Which kernel version is installed on the system? (Format: 1.22.3)

Answer: 4.15.0

Command: uname -r

Question: What is the name of the network interface that MTU is set to 1500?

Answer: ens192

Command: ifconfig | grep 1500

Navigation

Question: What is the name of the hidden "history" file in the htb-user's home directory?

Answer: .bash_history

Command: ls -a | grep history

Question: What is the index number of the "sudoers" file in the "/etc" directory?

Answer: 147627

Command: ls /etc/sudoers -i

Working with Files and Directories:

Question: What is the name of the last modified file in the "/var/backups" directory?

Answer: apt.extended_states.0

Command: ls -lt /var/backups | sed '2q;d'

Question: What is the inode number of the "shadow.bak" file in the "/var/backups" directory?

Answer: 265293

Command: ls /var/backups/shadow.bak -i | awk '{print $1}'

Find Files and Directories

Question: What is the name of the config file that has been created after 2020-03-03 and is smaller than 28k but larger than 25k?

Answer: 00-mesa-defaults.conf

Command: find / -type f -newermt 2020-03-03 -size +25k -size -28k -name "*.conf" -exec basename {} \; 2>/dev/null

Question: How many files exist on the system that have the ".bak" extension?

Answer: 4

Command: find / -type f -name "*.bak" 2>/dev/null | wc -l

Question: Submit the full path of the "xxd" binary.

Answer: /usr/bin/xxd

Command: which xxd

File Descriptors and Redirections:

Question: How many files exist on the system that have the ".log" file extension?

Answer: 32

Command: find / -type f -name "*.log" 2>/dev/null | wc -l

Question: How many total packages are installed on the target system?

Answer: 737

Command: dpkg --list | grep ^ii | wc -l

Filter Contents

Question: How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)

Answer: 7

Command: ss -l -4 | grep -v "127\.0\.0" | grep "LISTEN" | wc -l

(-l: listening services only

-4: ipv4 display only)

Question: Determine what user the ProFTPd server is running under. Submit the username as the answer.

Answer: Proftpd

Command: Option1: systemctl list-units --type=service --state=running | grep -i proftpd

Option2: ps aux | grep -i proftpd

(-i: case insensitive search)

System Management:

User Management

Question: Which option needs to be set to create a home directory for a new user using "useradd" command?

Answer: -m

Question: Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)

Answer: --lock

Question: Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option)

Answer: --command

Service and Process Management

Question: Use the "systemctl" command to list all units of services and submit the unit name with the description "Load AppArmor profiles managed internally by snapd" as the answer.

Answer: snapd.apparmor.service

Command: systemctl list-units --type=service | grep "Load AppArmor profiles managed internally by snapd" | awk '{print $1}'

Task Scheduling: Question:

What is the type of the service of the "syslog.service"?

Answer: notify

Command: systemctl show syslog.service -p Type