Linux System Hardening

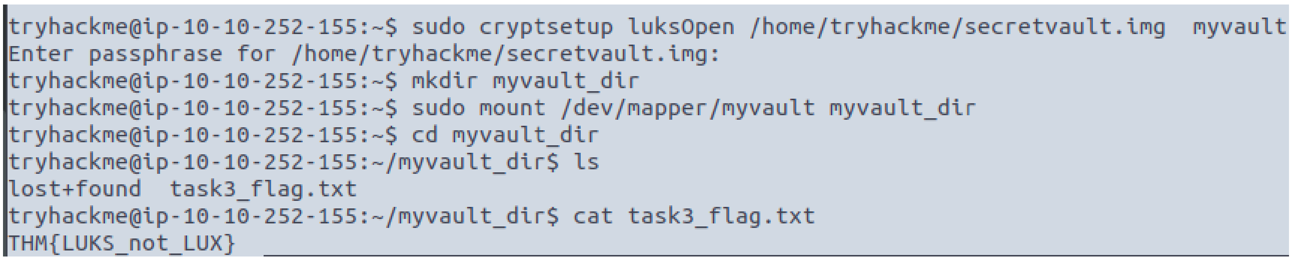
Task-1
No answer needed

Task-2
What command can you use to create a password for the GRUB bootloader?
grub2-mkpasswd-pbkdf2

What does PBKDF2 stand for?
Password-Based Key Derivation Function 2

Task-3
What does LUKS stand for?
Linux Unified Key Setup

We cannot attach external storage to the VM, so we have created /home/tryhackme/secretvault.img file instead. It is encrypted with the password 2N9EdZYNkszEE3Ad. To access it, you need to open it using cryptsetup and then mount it to an empty directory, such as myvault. What is the flag in the secret vault?
THM{LUKS_not_LUX}



```
tryhackme@ip-10-10-252-155:~$ sudo cryptsetup luksOpen /home/tryhackme/secretvault.img  myvault
Enter passphrase for /home/tryhackme/secretvault.img:
tryhackme@ip-10-10-252-155:~$ mkdir myvault_dir
tryhackme@ip-10-10-252-155:~$ sudo mount /dev/mapper/myvault myvault_dir
tryhackme@ip-10-10-252-155:~$ cd myvault_dir
tryhackme@ip-10-10-252-155:~/myvault_dir$ ls
lost+found  task3_flag.txt
tryhackme@ip-10-10-252-155:~/myvault_dir$ cat task3_flag.txt
THM{LUKS_not_LUX}
```

Task-4
There is a firewall running on the Linux VM. It is allowing port 22 TCP as we can ssh into the machine. It is allowing another TCP port; what is it?(sudo ufw status)
12526

What is the allowed UDP port?
14298

Task-5
What flag is hidden in the sshd_config file?
THM{secure_SEA_shell}

Task-6
One way to disable an account is to edit the passwd file and change the account's shell. What is the suggested value to use for the shell?
/sbin/nologin

What is the name of the RedHat and Fedora systems sudoers group?
wheel

What is the name of the sudoers group on Debian and Ubuntu systems?
sudo

Other than tryhackme and ubuntu, what is the username that belongs to the sudoers group?
Blacksmith

Task-7
Besides FTPS, what is another secure replacement for TFTP and FTP?
Sftp

Task-8
What command would you use to update an older Red Hat system?
yum update

What command would you use to update a modern Fedora system?
dnf update

What two commands are required to update a Debian system?
apt update && upgrade

What does yum stand for?
Yellowdog Updater, Modified

What does dnf stand for?
Dandified YUM

What flag is hidden in the sources.list file?
THM{not_Advanced_Persistent_Threat}

Task-9
What command can you use to display the last 15 lines of kern.log?
tail -n 15 kern.log

What command can you use to display the lines containing the word denied in the file secure?
grep denied secure

Task-10
No answer needed