ATTACK DEFENSE

by PentesterAcademy

Name	APT Repo: Preferences
URL	https://www.attackdefense.com/challengedetails?cid=1085
Type	Code Repository : APT Repository

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

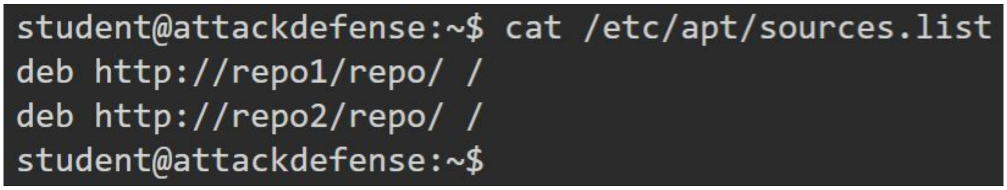
Two flags are hidden in "auditd" packages hosted on two different APT repositories (one flag in each package archive) on the same network. Your machine is configured to use these repositories.

Objective: Get the packages from both repositories and retrieve the flags!

Solution:

Step 1: Check the APT sources

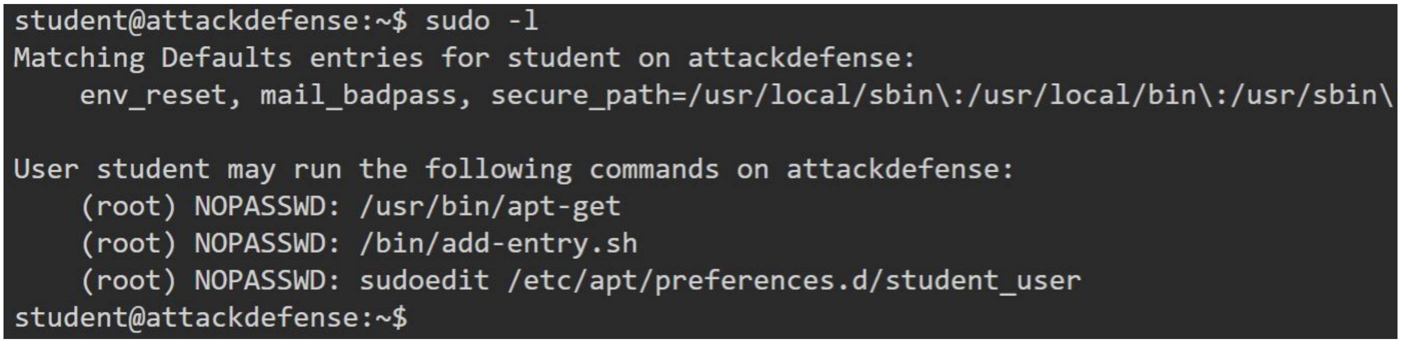
Command: cat /etc/apt/sources.list



```
student@attackdefense:~$ cat /etc/apt/sources.list
deb http://repo1/repo/ /
deb http://repo2/repo/ /
student@attackdefense:~$
```

Step 2: Check the sudo permissions granted to the user ‘student’.

Command: sudo -l

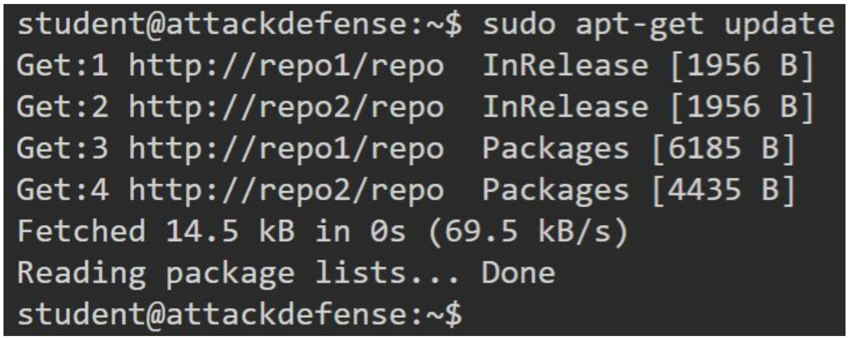


```
student@attackdefense:~$ sudo -l
Matching Defaults entries for student on attackdefense:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\

User student may run the following commands on attackdefense:
    (root) NOPASSWD: /usr/bin/apt-get
    (root) NOPASSWD: /bin/add-entry.sh
    (root) NOPASSWD: sudoedit /etc/apt/preferences.d/student_user
student@attackdefense:~$
```

Step 3: Update the apt-get configuration (including the sources)

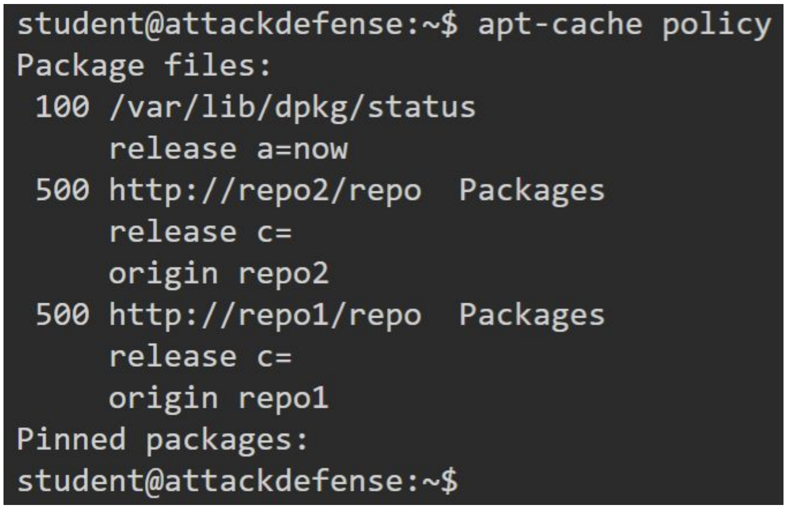
Command: sudo apt-get update



```
student@attackdefense:~$ sudo apt-get update
Get:1 http://repo1/repo  InRelease [1956 B]
Get:2 http://repo2/repo  InRelease [1956 B]
Get:3 http://repo1/repo  Packages [6185 B]
Get:4 http://repo2/repo  Packages [4435 B]
Fetched 14.5 kB in 0s (69.5 kB/s)
Reading package lists... Done
student@attackdefense:~$
```

Step 4: Check the apt-cache policy to see the preferences given to different sources/repositories.

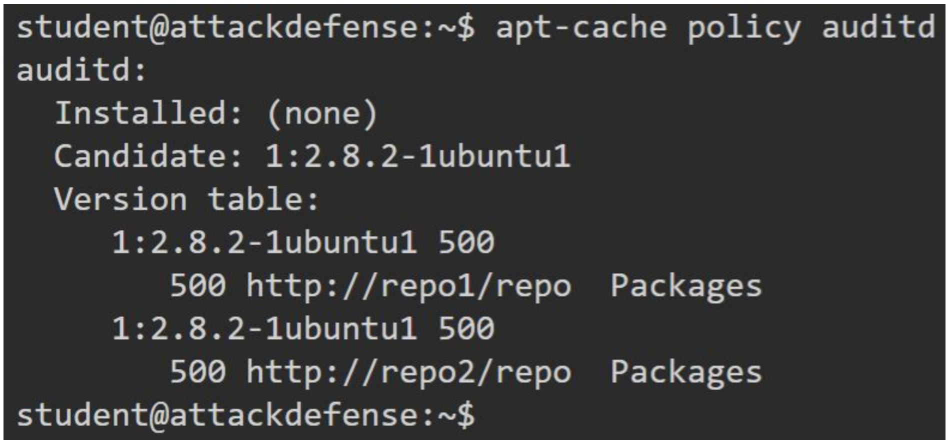
Command: apt-cache policy



```
student@attackdefense:~$ apt-cache policy
Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://repo2/repo  Packages
     release c=
     origin repo2
 500 http://repo1/repo  Packages
     release c=
     origin repo1
Pinned packages:
student@attackdefense:~$
```

Step 5: Check the apt-cache policy for auditd package.

Command: apt-cache policy auditd

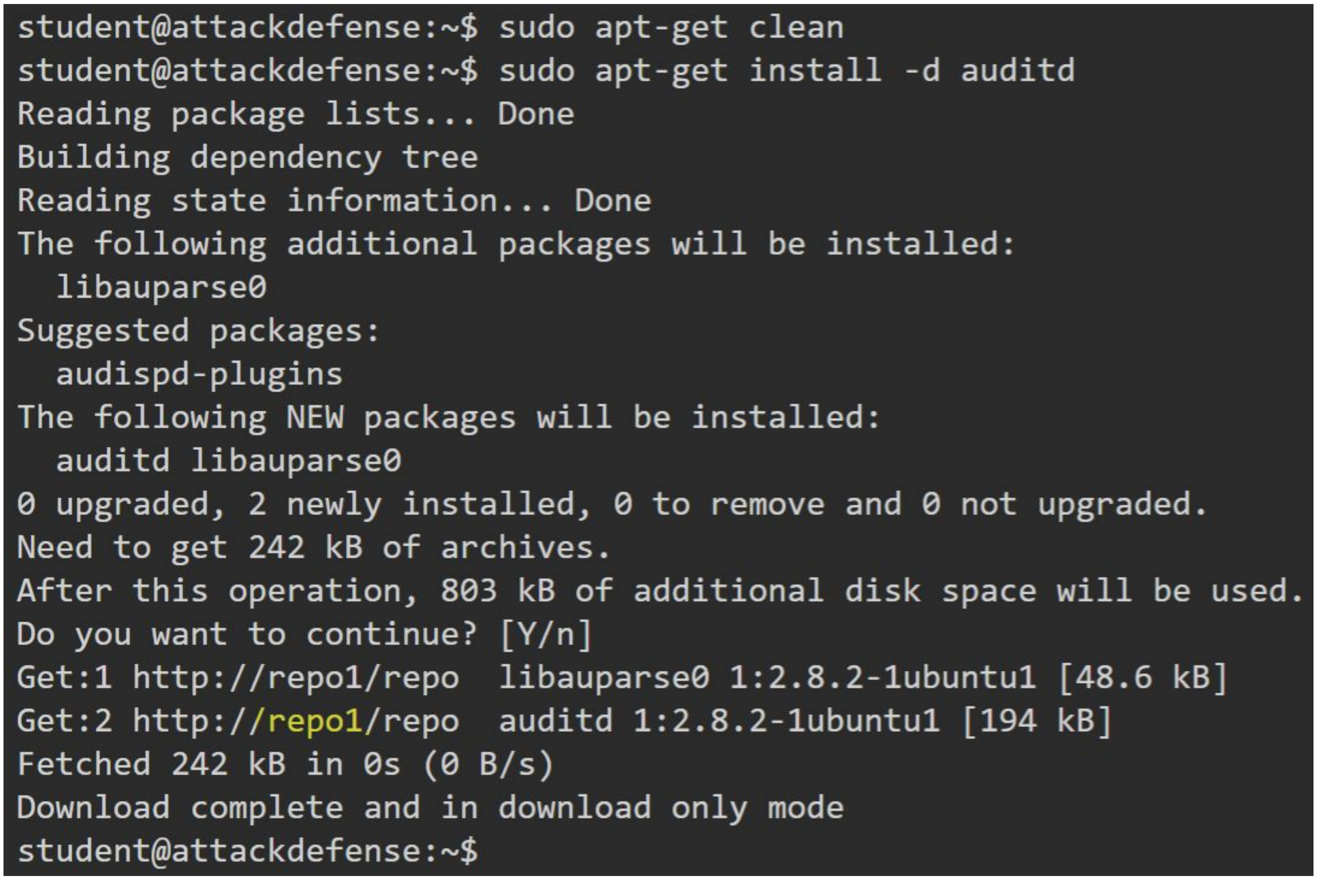


```
student@attackdefense:~$ apt-cache policy auditd
auditd:
  Installed: (none)
  Candidate: 1:2.8.2-1ubuntu1
  Version table:
     1:2.8.2-1ubuntu1 500
        500 http://repo1/repo  Packages
     1:2.8.2-1ubuntu1 500
        500 http://repo2/repo  Packages
student@attackdefense:~$
```

Step 6: The priority is same i.e. 500. Hence, for auditd package of same version, the package will be downloaded from repo1.

Clean the apt-cache and download the auditd package (not installing it).

Commands:
sudo apt-get clean
sudo apt-get install -d auditd



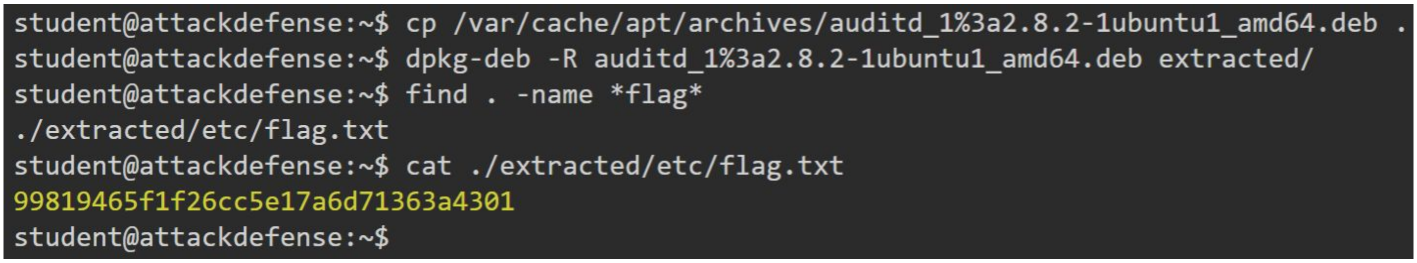
```
student@attackdefense:~$ sudo apt-get clean
student@attackdefense:~$ sudo apt-get install -d auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 242 kB of archives.
After this operation, 803 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://repo1/repo  libauparse0 1:2.8.2-1ubuntu1 [48.6 kB]
Get:2 http://repo1/repo  auditd 1:2.8.2-1ubuntu1 [194 kB]
Fetched 242 kB in 0s (0 B/s)
Download complete and in download only mode
student@attackdefense:~$
```

The package was downloaded from repo1.

Step 7: Copy the downloaded package to current directory, extracted it and retrieve the flag.

Commands:

```
cp /var/cache/apt/archives/auditd_1%3a2.8.2-1ubuntu1_amd64.deb .
dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted/
find . -name *flag*
cat ./extracted/etc/flag.txt
```



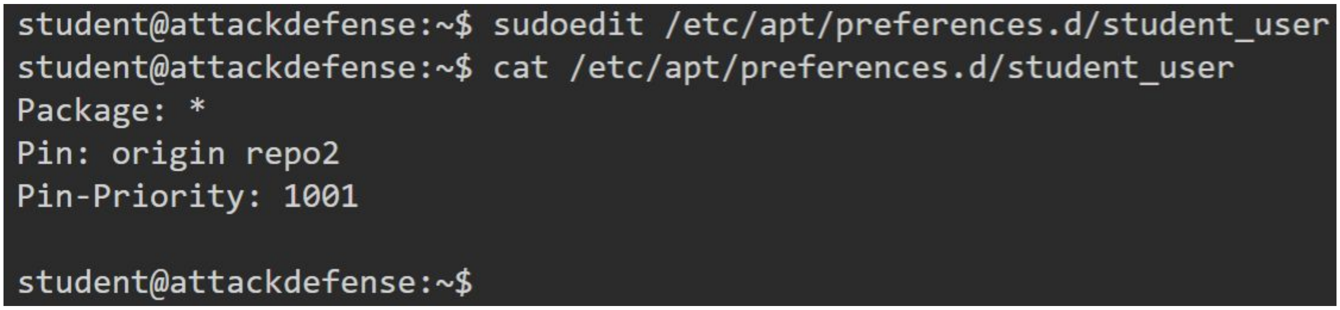
```
student@attackdefense:~$ cp /var/cache/apt/archives/auditd_1%3a2.8.2-1ubuntu1_amd64.deb .
student@attackdefense:~$ dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted/
student@attackdefense:~$ find . -name *flag*
./extracted/etc/flag.txt
student@attackdefense:~$ cat ./extracted/etc/flag.txt
99819465f1f26cc5e17a6d71363a4301
student@attackdefense:~$
```

Flag1: 99819465f1f26cc5e17a6d71363a4301

Step 8: The student user also has permission to edit or create apt preference config file. Create the file with the following content.

Commands:
sudoedit /etc/apt/preferences.d/student_user
cat /etc/apt/preferences.d/student_user

Content:
Package: *
Pin: origin repo2
Pin-Priority: 1001

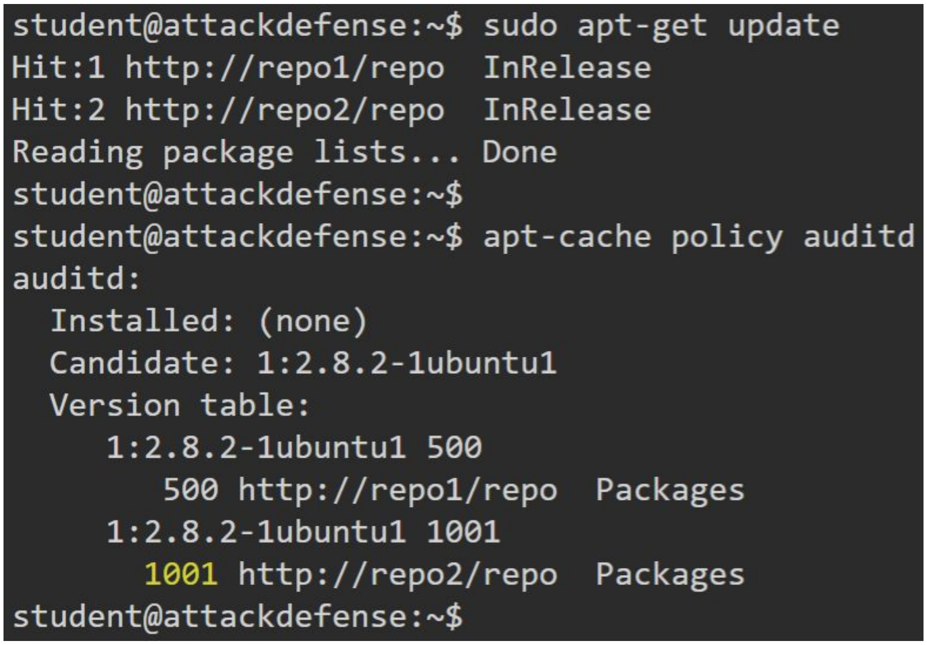


```
student@attackdefense:~$ sudoedit /etc/apt/preferences.d/student_user
student@attackdefense:~$ cat /etc/apt/preferences.d/student_user
Package: *
Pin: origin repo2
Pin-Priority: 1001

student@attackdefense:~$
```

Step 9: Update the apt configuration and check the apt-cache policy again.

Commands:
sudo apt-get update
apt-cache policy auditd

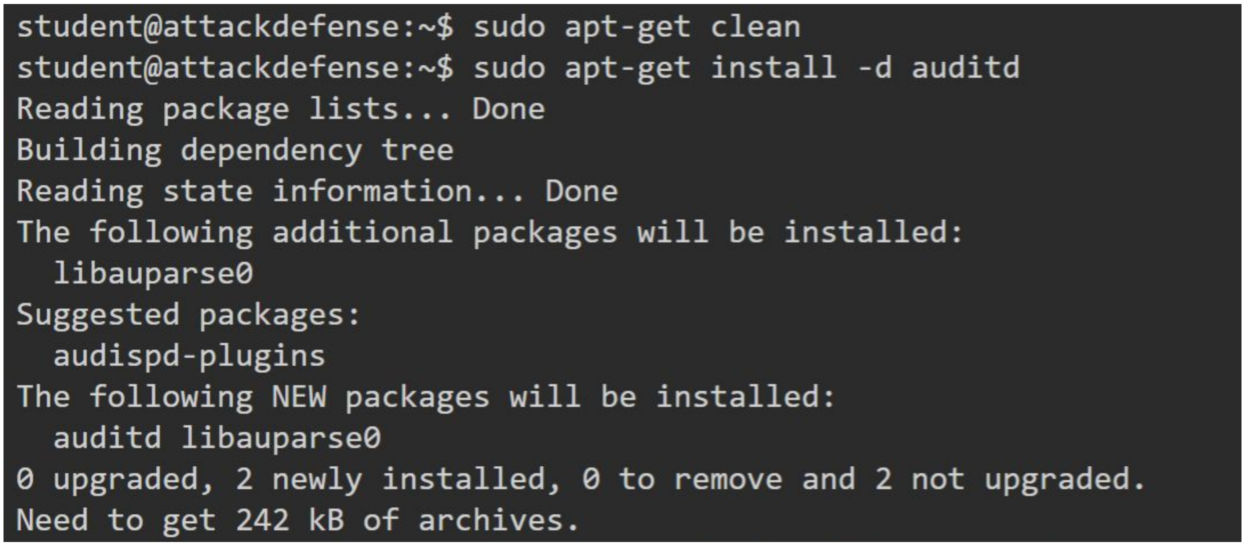


```
student@attackdefense:~$ sudo apt-get update
Hit:1 http://repo1/repo  InRelease
Hit:2 http://repo2/repo  InRelease
Reading package lists... Done
student@attackdefense:~$
student@attackdefense:~$ apt-cache policy auditd
auditd:
  Installed: (none)
  Candidate: 1:2.8.2-1ubuntu1
  Version table:
     1:2.8.2-1ubuntu1 500
        500 http://repo1/repo  Packages
     1:2.8.2-1ubuntu1 1001
       1001 http://repo2/repo  Packages
student@attackdefense:~$
```

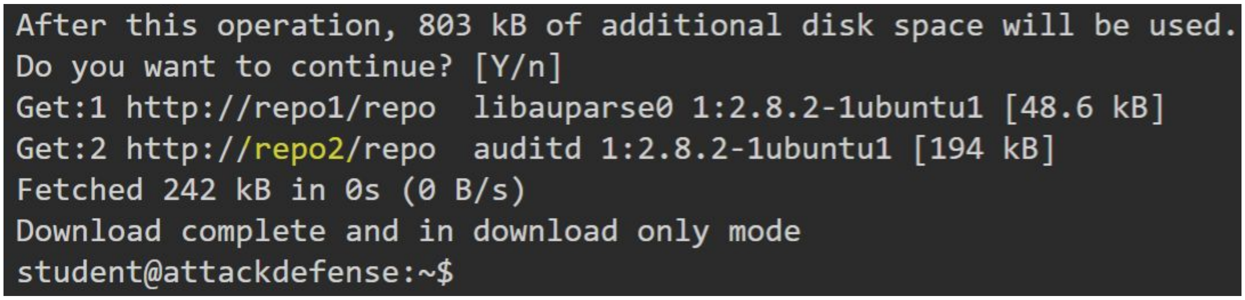
Step 10: The repo2 is given higher priority, hence the package will be downloaded from repo2. Clean the apt-cache and download the auditd package (not installing it).

Commands:

sudo apt-get clean
sudo apt-get install -d auditd



```
student@attackdefense:~$ sudo apt-get clean
student@attackdefense:~$ sudo apt-get install -d auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 242 kB of archives.
```



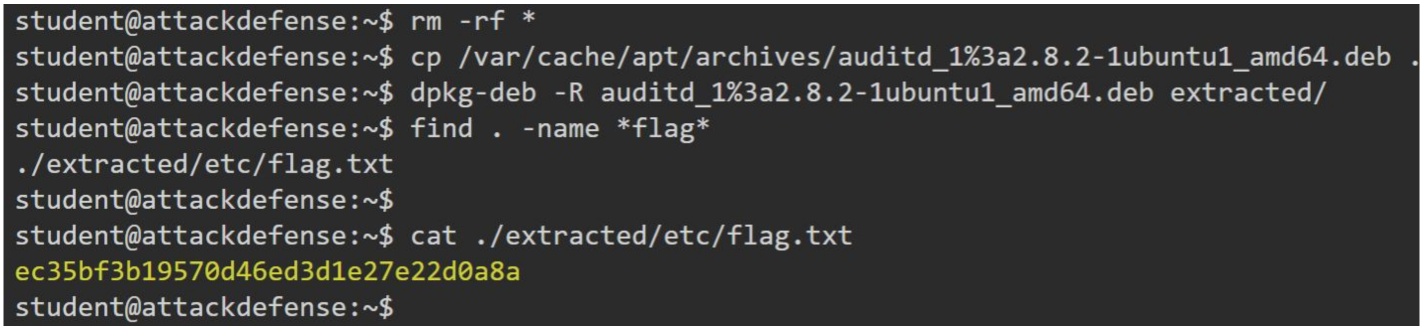
```
After this operation, 803 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://repo1/repo  libauparse0 1:2.8.2-1ubuntu1 [48.6 kB]
Get:2 http://repo2/repo  auditd 1:2.8.2-1ubuntu1 [194 kB]
Fetched 242 kB in 0s (0 B/s)
Download complete and in download only mode
student@attackdefense:~$
```

The package was downloaded from repo2.

Step 11: Copy the downloaded package to current directory, extracted it and retrieve the flag.

Commands:

```
cp /var/cache/apt/archives/auditd_1%3a2.8.2-1ubuntu1_amd64.deb .
dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted/
find . -name *flag*
cat ./extracted/etc/flag.txt
```



```
student@attackdefense:~$ rm -rf *
student@attackdefense:~$ cp /var/cache/apt/archives/auditd_1%3a2.8.2-1ubuntu1_amd64.deb .
student@attackdefense:~$ dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted/
student@attackdefense:~$ find . -name *flag*
./extracted/etc/flag.txt
student@attackdefense:~$
student@attackdefense:~$ cat ./extracted/etc/flag.txt
ec35bf3b19570d46ed3d1e27e22d0a8a
student@attackdefense:~$
```

Flag2: ec35bf3b19570d46ed3d1e27e22d0a8a

References:

1. apt-get (https://linux.die.net/man/8/apt-get)
2. APT package manager (https://en.wikipedia.org/wiki/APT_(Package_Manager))
3. APT preferences (http://manpages.ubuntu.com/manpages/disco/en/man5/apt_preferences.5.html)