Overview:

CVE triage is the process of evaluating CVEs and determining whether they affect Ubuntu.

The password for the VM you have been given is 'ubuntu'. Please change it upon logging in.

There is a new Ubuntu release every 6 months. The ubuntu version number indicates the year and month of release. For example, 18.04 Bionic Beaver was released in April of 2018. LTS stands for "Long Term Support". Every 2 years an LTS release is produced. LTS releases are supported for 5 years. At the time of this writing, 16.04 Xenial, 18.04 Bionic, and 20.04 Focal are the current LTS releases. 20.10 Groovy will be released in October and supported until July of 2021.

The Ubuntu package repository is split up into 4 components. Of specific interest are:
main: Officially supported
universe: Community maintained and supported
https://askubuntu.com/questions/58364/whats-the-difference-between-multiverse-universe-restricted-and-main

To start analyzing/triaging CVEs, you'll need to pull the Ubuntu CVE Tracker git repository. This has already been done in the VM provided to you (cd $UCT). It would be valuable to read $UCT/README.

Next, you can take a look at the list of all CVEs that affect packages in the universe (community) component. This web page shows the status of each CVE for each package it affects for each currently supported Ubuntu release.

Choose a CVE you think may be incorrectly triaged. The biggest indicator of this is if the status for any release is, "needs-triage". Use a text editor to open the CVE's file at $UCT/active/CVE-YEAR-\d{4,}

You can use the command `umt search PACKAGE` to list the package's version for every currently supported version of Ubuntu. In order to determine whether or not the package is affected for a given Ubuntu release, you can compare the package's version to:

1) Version numbers listed in the CVE
2) Version numbers in the Debian security tracker
3) Version numbers in any links that may be present in the CVE file

Debian version numbers:

Debian version numbers are formatted like:
[epoch]:upstream_version[-debian_revision]
http://www.fifi.org/doc/debian-policy/policy.html/ch-versions.html

in a version like "1:2.3.4-5",
epoch = 1
upstream_version = 2.3.4
debian_revision = 5

If you see versions that look like this, "1.7.4-2+deb9u1", the "+deb9u2" indicates that there have been 2 security fixes for this package in Debian 9.

If you see versions that look like this, "1.7.4-2ubuntu0.1", this indicates there has been 1 ubuntu security fix. In general, "ubuntu\d" indicates there is an ubuntu specific change, and "ubuntu\d.\d" indicates there has been a security fix and/or an ubuntu-specific change to the package.

You can compare package versions using the following command:
dpkg --compare-versions "VERSION_1" gt "VERSION_2" && echo "true" || echo "false"
Note that gt = "Greater Than". You can also supply "eq", "ge", "lt", and "le". See `man dpkg` for more information.

You can download the source code of the package by doing `umt download PACKAGE`.
Comparing the commits that fix the issue to the code in the package can be very helpful in determining whether or not the package is affected.

If the package is affected, change its status to "needed". If it is not affected, change its status to "not-affected (REASON)". The reason might be the version number of the package or something such as "code not present".

Please note that some projects maintain multiple versions of their software simultaneously. Therefore, you cannot just assume that if a fix was released for version

1.1, all greater versions (e.g. 2.0) are fixed. For example, a project may maintain a 1.x and 2.x version of the software. The vulnerability may be fixed in v1.1 and v2.1. Therefore, even though v2.0 > v1.1, it is still vulnerable.

Example:

Evaluate CVE-2018-13440. This CVE affects the package "audiofile". Using `umt search audiofile`, we can see the versions of the audiofile packages corresponding to reach Ubuntu release:

```
trusty: 0.3.6-2ubuntu0.14.04.3, Pocket: updates, Component: main
xenial: 0.3.6-2ubuntu0.16.04.1, Pocket: updates, Component: universe
bionic: 0.3.6-4, Pocket: release, Component: universe
eoan: 0.3.6-5, Pocket: release, Component: universe
focal: 0.3.6-5build1, Pocket: release, Component: universe
```

By looking at the debian security tracker (https://security-tracker.debian.org/tracker/CVE-2018-13440), we can see that the following two versions are fixed in debian: 0.3.6-4+deb9u1, and 0.3.6-5.

Comparing these versions to the ubuntu versions, we can surmise that the status of xenial, and bionic should be "needed", while the status of eoan and focal should be "not-affected (0.3.6-5)". A fix for trusty has already been released. After triage, the diff of $UCT/active/CVE-2018-13440 would look like:

```
diff --git a/active/CVE-2018-13440 b/active/CVE-2018-13440
index e2da705178..aef3968463 100644
--- a/active/CVE-2018-13440
+++ b/active/CVE-2018-13440
@@ -30,10 +30,10 @@ upstream_audiofile: needs-triage
 precise/esm_audiofile: DNE
 trusty_audiofile: released (0.3.6-2ubuntu0.14.04.3)
 trusty/esm_audiofile: released (0.3.6-2ubuntu0.14.04.3)
-xenial_audiofile: needs-triage
+xenial_audiofile: needed
 artful_audiofile: ignored (reached end-of-life)
-bionic_audiofile: needs-triage
+bionic_audiofile: needed
```

cosmic_audiofile: ignored (reached end-of-life)
disco_audiofile: ignored (reached end-of-life)
-eoan_audiofile: needs-triage
-devel_audiofile: needs-triage
+eoan_audiofile: not-affected (0.3.6-5)
+devel_audiofile: not-affected (0.3.6-5)

Note that the version listed next to "not-affected" for all Ubuntu releases is the first version of the package that was not affected.