Lab 1 part 2
50 Points
Due:April 5

Lab 1 part 2 is broken up into two different parts, A and B, which are worth 25 points each.

1 Part A:

Give an overview of the events that transpired on groucho. For example: what order did users add themselves, what sorts of mischief were various users up to?

2 Part B:

Declare whether you will convict or defend the student Matt Barney of his heinous crimes against the class. He is accused of corrupting the SSH configuration files such that the SSH server on groucho became unavailable.Make your case using as much evidence as possible. You may also find and implicate another culprit if you wish.

3 Turn in

Write up parts A and B with no more than a page each(2 pages total).You should have a separate "evidence" file of which your write up references. Turn in a PDF file of your write up along with a compressed evidence file (evidence.tar.gz) to the address specified in the syllabus.

4 Tips

Start by examining what's in "/var/log/". Then look at "~/bash_history" of each user.