Jed's thoughts on Werewolves, Spring 2017

What I would have done

- ltrace and strace of sshd to steal passwords as root on your own VM
  - chage -d 0 username (make them pick their own password)
  - http://pentestmonkey.net/blog/sshd-snooping
- Deal with noise in side channels by monitoring both the server and client processes, and correlating
  - pipe transitions, context switches, pty devices, etc.
- Burglary and blackmail not okay as per University rules, but I might have authorized bribery of members of other groups (but not me, SSG, or the TA)

Other ideas...

- Keyboard acoustic emanations
  - I have source code somewhere...
- ARP spoofing
  - During setup
  - During initial logins before the first game
- Stupid stuff
  - “[sudo] password for moderator:”
  - “Hey look, the server filters out your password if you try to share it: ********”
  - “We set our root password to the password of a sudoer on another group's server, figured we'd give you a chance at revenge”

If you don't mind, send me...

- Source code
- Commands
- Instructions
- Bug reports
- General feedback
- ...anything you think would be helpful to make Werewolves or the lab better in the future
  - (Same is true of the other labs and class in general)