# Group1 Werewolves Lab

## Lessons Learned

Miri Ryu, Tyler Shelton, Don Owen*, Guoshun Yang, Xuan Yu

# Things we tried and failed at, or noticed but didn’t try

- Tried to trick the TA into giving us other another groups passwords (Good job Nidia)
- Exploiting the `nvaquera` or `crandall` accounts - sudo access on all servers that didn’t disable them, used the same password on every server
  - Thought about hashcat, decided it probably wasn’t worth the time
- Every ssh server private key was identical, possibility to impersonate another server by changing IPs
  - Bunch of other stuff duplicated too, looks like there was one master VM image and then cloned 60x

# Lesson 0x01: With enough grep, anything is possible

TCP/IP exploit all in one bash line, automatically prints a user name when they type (but noisy)

```
while : ;  do who --ips > ips.log; netstat -an --timer | grep ":22" | grep "(0" | grep "on" | grep -v LISTEN | tr -s ' ' | cut -d" " -f5 | cut -d":" -f1 | xargs grep ips.log -e 2> /dev/null | cut -d" " -f1; sleep 0.01; done;
```

# Lesson 0x02 Don’t leave your passwords visible

- Sorry group8 and the .179 server!
- Had root access a month ago
- Backdoored with
  - ssh keys we controlled for root
  - ssh keys we controlled for cs444
  - SETUID bit on /bin/nano (edit anything without root, like sudoers file)

# Lesson 0x03 Don’t leave your passwords visible (revisited)

- The .169 server (intentionally) left a file list with group9 password=”password” and with group9 sudo access
- Used command injection to get to the file
- Get password, change password (lock others out), have root

# Nefarious root things (sorry again)

- su as anyone - impersonate anyone, including moderator, vote for them, replace their messages with yours
- Change game settings
- Impersonate moderator and tell groups to do certain things
- View any log file any time
- Kill processes…
- The sky's the limit

# Lesson 0x04 : Don’t make weak passwords (seeing a theme here?)

- On group0’s server, passwords were predictable - fruits in alphabetical order, lowercase, singular
- Guessed other groups passwords, impersonated them, run a second client.py as them, type for them
- Passwords!
  Group1 - banana, Group2 - cherry, Group3 - date, Group4 - fig, Group5 - grape, Group6 - honey, Group7 - kiwi