## Activity File: Linux Scavenger Hunt

In this activity you can work alone or in teams to complete the challenge.

If you are working on a team, every team member must participate and work at least one task. Think of this as a relay race with each teammate helping out.

To complete this challenge, you will launch a a headless virtual machine server and login.

All previous class material and internet resources are fair game.

Each team member can work on a different step, but most steps must be completed in order.

Professors and TA‚Äôs will not be giving hints or assistance unless there are issues with getting the virtual machine to run correctly.

\*\*Hints:\*\*

- Take notes of anything you find interesting.

- When you find a flag, you will see this format `flag\_1:97df27aec8c251503f5e3749eb2ddea2`. Make a note of where you found each flag.

- Find 8 flags in total. 7 flags from the system combine to make up the final flag.

- Write down any credentials that you find so you don't have to try to remember them and you won't have to retrace any steps you've already completed.

### Instructions

In order to create your scavenger hunt VM and connect to it, read and execute the following instructions.

\*\*NOTE:\*\* Complete the following instructions on your \_\*\*personal computer\*\*\_ and \_\*\*NOT WITHIN\*\*\_ the virtual machines you have been using for classes thus far.

To get this new Linux server to run in their lab environment, log in and open `Git Bash` if you are using a PC or open Terminal if you are using a Mac.

Open your personal computer's `Git Bash` / Mac terminal.

Run this command using `Git Bash`:

- `curl -s -L https://tinyurl.com/yaac2lnz | bash`

- This command may take several minutes to run.

\*\*Note\*\*: If you run the script and get an OpenSSL error and can‚Äôt download the VM, you should just run the script again ‚Äî this occasionally happens but is just an intermittent network issue and goes away if you retry

The output should be \_similar\_ to:

```bash

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 816 0 816 0 0 3487 0 --:--:-- --:--:-- --:--:-- 3502

100 1169 100 1169 0 0 3510 0 --:--:-- --:--:-- --:--:-- 3510

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 1831 100 1831 0 0 15649 0 --:--:-- --:--:-- --:--:-- 15649

Cloning into 'C:/Documents/LabEnvironments/linux-scavenger'...

remote: Enumerating objects: 55, done.

remote: Counting objects: 100% (55/55), done.

remote: Compressing objects: 100% (27/27), done.

remote: Total 55 (delta 32), reused 47 (delta 27), pack-reused 0

Receiving objects: 100% (55/55), 6.50 KiB | 951.00 KiB/s, done.

Resolving deltas: 100% (32/32), done.

Submodule 'linux-scavenger-hunt-vm' (git@gitlab.com:cyberxsecurity/virtual-machines/linux-scavenger-hunt-vm.git) registered for path 'linux-scavenger-hunt-vm'

Submodule 'reprovision' (git@gitlab.com:cyberxsecurity/flux/reprovision.git) registered for path 'reprovision'

Cloning into 'C:/Documents/LabEnvironments/linux-scavenger/linux-scavenger-hunt-vm'...

Cloning into 'C:/Documents/LabEnvironments/linux-scavenger/reprovision'...

Submodule path 'linux-scavenger-hunt-vm': checked out 'cd0ff2c42fec17aeb2d7d65250d539ac9412da18'

Submodule path 'reprovision': checked out '34c97a8d086f26612a61bfaaafd95bb975c968aa'

Bringing machine 'linux' up with 'hyperv' provider...

==> linux: Verifying Hyper-V is enabled...

==> linux: Verifying Hyper-V is accessible...

==> linux: Box 'cybersecurity/linux-scavenger' could not be found. Attempting to find and install...

linux: Box Provider: hyperv

linux: Box Version: >= 0

==> linux: Loading metadata for box 'cybersecurity/linux-scavenger'

linux: URL: https://vagrantcloud.com/cybersecurity/linux-scavenger

==> linux: Adding box 'cybersecurity/linux-scavenger' (v1.0.1582326967) for provider: hyperv

linux: Downloading: https://vagrantcloud.com/cybersecurity/boxes/linux-scavenger/versions/1.0.1582326967/providers/hyperv.box

linux: Download redirected to host: vagrantcloud-files-production.s3.amazonaws.com

linux:

==> linux: Successfully added box 'cybersecurity/linux-scavenger' (v1.0.1582326967) for 'hyperv'!

==> linux: Importing a Hyper-V instance

linux: Creating and registering the VM...

linux: Successfully imported VM

linux: Configuring the VM...

==> linux: Starting the machine...

==> linux: Waiting for the machine to report its IP address...

linux: Timeout: 120 seconds

linux: IP: 127.0.0.1

==> linux: Waiting for machine to boot. This may take a few minutes...

linux: SSH address: 127.0.0.1:2200

linux: SSH username: vagrant

linux: SSH auth method: private key

==> linux: Machine booted and ready!

Connect via SSH by running:

ssh student@192.168.100.105

```

Run the ssh command shown in the output.

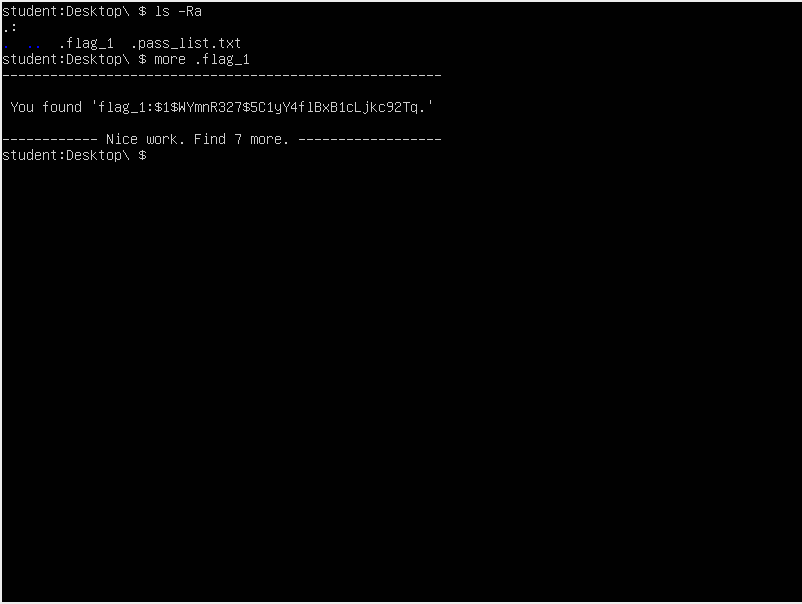
Login with `student:Goodluck!`

---

### flag\_1:

Finding this flag is imperative to moving on quickly, as it contains the passwords from users before they were hacked. Luckily, it doesn't have a great hiding spot.

ls -Ra



### flag\_2:

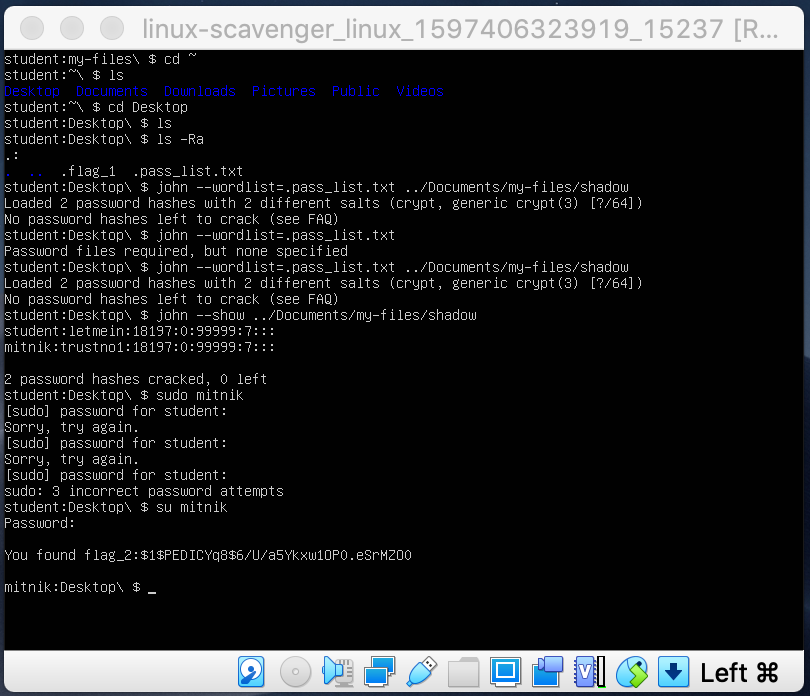
A famous hacker had created a user on the system a year ago. Find this user, crack his password and login to his account.

john –-wordlist=.pass\_list.txt

john –-wordlist=.pass\_list.txt ../Documents/my-files/shadow

su mitnik

trustno1



### flag\_3:

Find a ‚Äòlog‚Äô file \_and\_ a zip file related to the hacker's name.

- Use a compound command to figure out the unique count of IP Addresses in this log file. That number is a password.

- \*\*Hint:\*\* Use the `unzip` command to open any zip files you may find.

- Note: To unzip the zip file, use the `unzip` command.

cd ~

cd /var/log/mitnik.log

cat /var/log/mitnik.log | sort | uniq | wc -l

cd ~

cd /home/Documents/

ls

unzip .secret.zip

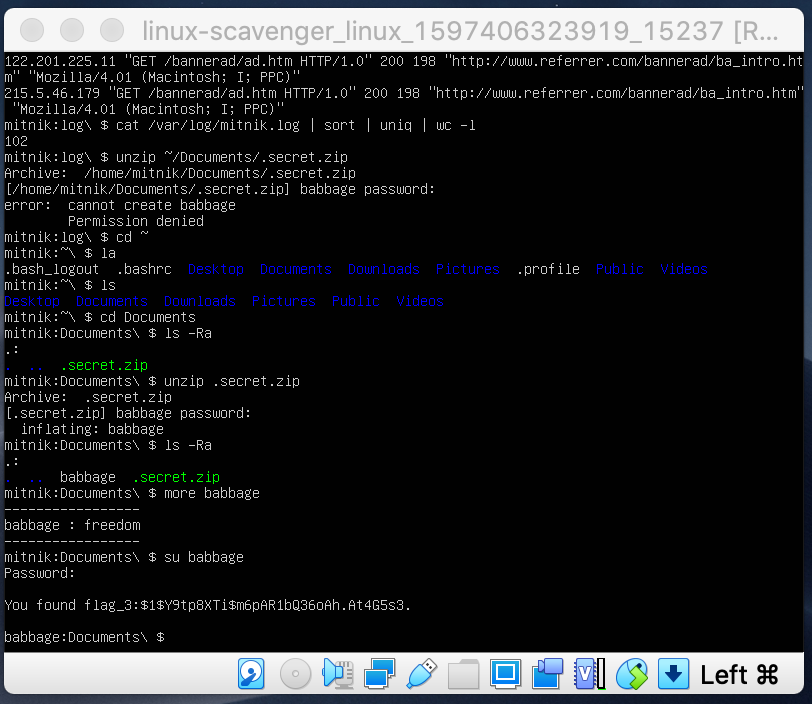
password: 102

ls

more babbage

su babbage

password: freedom



### flag\_4:

Find a directory with a list of hackers. Look for a file that has `read` permissions for the owner, `no` permissions for groups and `executable` only for everyone else.

cd ~

cd /home/

ls -Ra

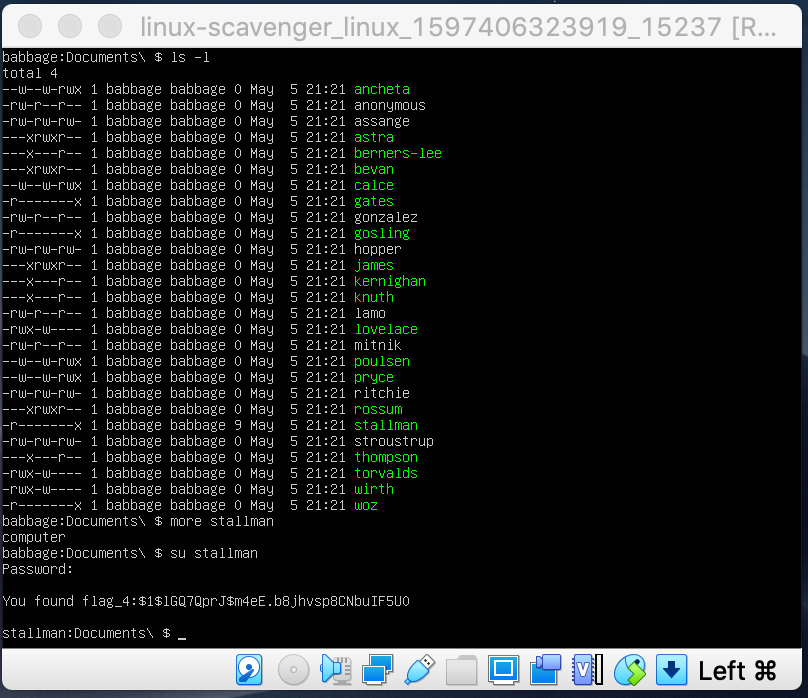
cd /Documents

ls -l

more stallman

su stallman

password: computer



### flag\_5:

This user is writing a bash script, except it isn't quite working yet. Find it, debug it and run it.

Cd ~

Cd /Documents

ls -Ra

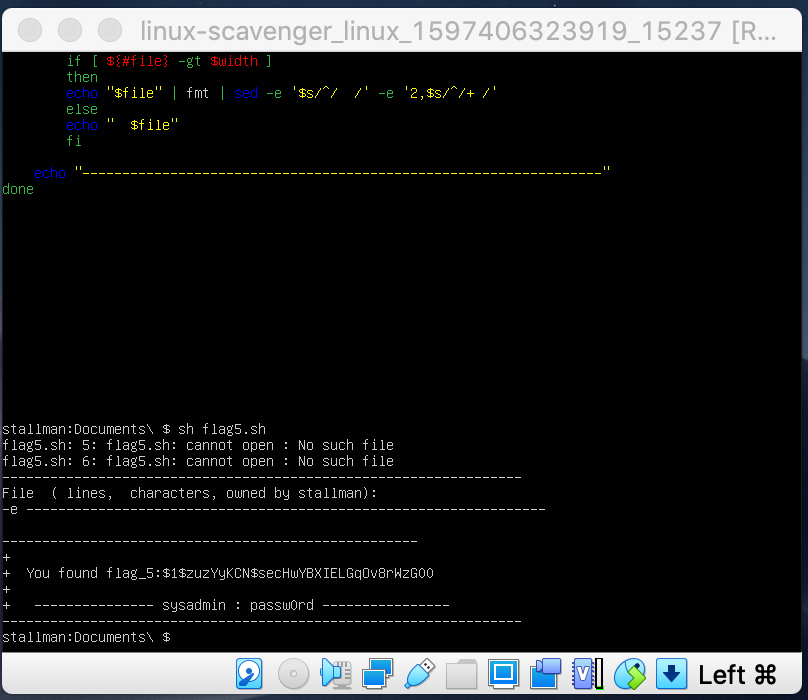
chmod +x flag5.sh

sh flag5.sh

sysadmin + passw0rd

su sysadmin

password: passw0rd



### flag\_6:

Inspect this user's custom aliases and run the suspicious one for the proper flag.

Su sysadmin

Alias

