Linux Review

Cybersecurity

Review Week Day 3

Class Objectives

In today's class, we will review Linux by:

- Using `awk` and `sed` to parse text files.
- Locating files on disk with `find`.
- Setting and interpreting file permissions.
- Using `su` and `sudo` to manipulate privileges on a Linux machine.

General Linux Review

Your Turn: General Linux Review

In this activity, you will review Linux concepts, directories and commands.

Feel free to work with a partner. If you want to use this activity to gauge your Linux knowledge, you can also work solo.

Once finished, we will review each question as a class.

Files sent via Slack.

Suggested Time:
25 Minutes

Times Up! Let’s Review.

Linux Review

General Review

What are some Text Editors?

What is the top of the Linux file structure?

General Review

What are some Text Editors?

`nano, vim, and emacs`

What is the top of the Linux file structure?

General Review

What are some Text Editors?

`nano, vim, and emacs`

What is the top of the Linux file structure?

`/`

General Review

Name the directories that contain:

Binaries: _____

Files associated to the Kernel: _____

Log Files: _____

Temporary Files: _____

Configuration Files: _____

Process Files: _____

Files the user wants to save: _____

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: _____

Log Files: _____

Temporary Files: _____

Configuration Files: _____

Process Files: _____

Files the user wants to save: _____

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: _____

Temporary Files: _____

Configuration Files: _____

Process Files: _____

Files the user wants to save: _____

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: `/var/log`

Temporary Files: _____

Configuration Files: _____

Process Files: _____

Files the user wants to save: _____

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: `/var/log`

Temporary Files: `/tmp, /var/tmp`

Configuration Files: `_______`

Process Files: `_______`

Files the user wants to save: `_______`

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: `/var/log`

Temporary Files: `/tmp, /var/tmp`

Configuration Files: `/etc/`

Process Files: `_______`

Files the user wants to save: `_______`

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: `/var/log`

Temporary Files: `/tmp, /var/tmp`

Configuration Files: `/etc/`

Process Files: `/proc`

Files the user wants to save: `_______`

General Review

Name the directories that contain:

Binaries: `/bin, /usr/bin, /usr/sbin`

Files associated to the Kernel: `/boot`

Log Files: `/var/log`

Temporary Files: `/tmp, /var/tmp`

Configuration Files: `/etc/`

Process Files: `/proc`

Files the user wants to save:`/home`

General Review

Name the commands you use to:

Install a package: _____

Add a user: _____

Change a password: _____

Create a new group: _____

Add a user to a group: _____

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: _____

Change a password: _____

Create a new group: _____

Add a user to a group: _____

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: _____

Create a new group: _____

Add a user to a group: _____

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: `passwd <user>`

Create a new group: _____

Add a user to a group: _____

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: `passwd <user>`

Create a new group: `groupadd <group>`

Add a user to a group: _____

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: `passwd <user>`

Create a new group: `groupadd <group>`

Add a user to a group: `usermod -aG <group> <username>`

Check which groups you're in:_____

Find your user ID: _____

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: `passwd <user>`

Create a new group: `groupadd <group>`

Add a user to a group: `usermod -aG <group> <username>`

Check which groups you're in: `groups`

Find your user ID: _______

General Review

Name the commands you use to:

Install a package: `apt install <package>`

Add a user: `adduser, useradd`

Change a password: `passwd <user>`

Create a new group: `groupadd <group>`

Add a user to a group: `usermod -aG <group> <username>`

Check which groups you're in: `groups`

Find your user ID: `id`

General Review

What are the three types of file permissions?

Which command displays a file’s permissions?

Which file gets modified when a user is added to the system?

Which file contains hashed passwords?

General Review

What are the three types of file permissions?

Owner, Group, and World/Other

Which command displays a file’s permissions?

Which file gets modified when a user is added to the system?

Which file contains hashed passwords?

General Review

What are the three types of file permissions?

Owner, Group, and World/Other

Which command displays a file's permissions?

`ls -l <filename>`

Which file gets modified when a user is added to the system?

Which file contains hashed passwords?

General Review

What are the three types of file permissions?

Owner, Group, and World/Other

Which command displays a file's permissions?

`ls -l <filename>`

Which file gets modified when a user is added to the system?

`/etc/passwd`

Which file contains hashed passwords?

General Review

What are the three types of file permissions?

Owner, Group, and World/Other

Which command displays a file's permissions?

`ls -l <filename>`

Which file gets modified when a user is added to the system?

`/etc/passwd`

Which file contains hashed passwords?

`/etc/shadow`

General Review

How can you tell which algorithm was used to hash a password?

Which command changes file permissions?

What are the two ways to change file permissions?

What is the command to change ownership permissions?

General Review

How can you tell which algorithm was used to hash a password?

Look at the number in the dollar sign. (6 = sha512-crypt hash)

Which command changes file permissions?

What are the two ways to change file permissions?

What is the command to change ownership permissions?

General Review

How can you tell which algorithm was used to hash a password?

Look at the number in the dollar sign. (6 = sha512-crypt hash)

Which command changes file permissions?

`chmod`

What are the two ways to change file permissions?

What is the command to change ownership permissions?

General Review

How can you tell which algorithm was used to hash a password?

Look at the number in the dollar sign. (6 = sha512-crypt hash)

Which command changes file permissions?

`chmod`

What are the two ways to change file permissions?

Symbolic and octal

What is the command to change ownership permissions?

General Review

How can you tell which algorithm was used to hash a password?

Look at the number in the dollar sign. (6 = sha512-crypt hash)

Which command changes file permissions?

`chmod`

What are the two ways to change file permissions?

Symbolic and octal

What is the command to change ownership permissions?

`chown`

General Review

How do you edit the sudoers file?

How do you use sudo?

What is the command to switch to another user?

What is the command to archive a file?

General Review

How do you edit the sudoers file?

`visudo`

How do you use sudo?

What is the command to switch to another user?

What is the command to archive a file?

General Review

How do you edit the sudoers file?

`visudo`

How do you use sudo?

`sudo <command>`

What is the command to switch to another user?

What is the command to archive a file?

General Review

How do you edit the sudoers file?

`visudo`

How do you use sudo?

`sudo <command>`

What is the command to switch to another user?

`su`

What is the command to archive a file?

General Review

How do you edit the sudoers file?

`visudo`

How do you use sudo?

`sudo <command>`

What is the command to switch to another user?

`su`

What is the command to archive a file?

`tar cvf <archive name> <file>`

General Review

What is the command to view running processes?

Which two commands can be used to kill processes? Which one requires PID?

General Review

What is the command to view running processes?

Top lists them dynamically. **ps** lists them statically.

Which two commands can be used to kill processes? Which one requires PID?

General Review

What is the command to view running processes?

Top lists them dynamically. **ps** lists them statically.

Which two commands can be used to kill processes? Which one requires PID?

`kill <PID> and killall <Process Name>. Only kill requires PID.`

Reintroduction to AWK

Introduction to AWK

Awk is a programming language designed specifically for processing text.

While AWK can be used to create entire text processing programs, it can also be used directly in the command line to do quick and useful tasks.

```
awk '{print}' celeb_emails.txt
```

- `awk` invokes the `awk` program
- `'{ }'` wraps around the `awk program` that you will run.
- `print` is `awk's` print command.

This command is the same as `awk `{print $0}' celeb_emails.txt`

Awk

Like Sed, the awk program located inside the `{ }` is run on each line of a text file.

- **`$0`** is awk's variable that holds value of each line.
- Awk also assigns variables to each field in each line.
  - By default, awk uses any white space it comes across to define a field.
  - $1 is used for the first field, $2 for the second, and so on.

For example, run: `awk '{print $3, $2, $4}' celeb_emails.txt`

Awk: -F flags and regex

The `-F` flag for awk allows you to change the delimiter that awk is using to separate fields.

```
awk -F, `{print $1}` celeb_emails.txt
```

Regular expressions (regex) work in awk the same way they work in `sed`.

- `//` holds the search string or regex

`For example:`

- `awk `/Celebrity_Name/` celeb_emails.txt` to print out the lines that contain the name you are searching for.
- `awk '/aol/' celeb_emails.txt` to print only the aol emails.

Your Turn: Start gAWK-ing

In this activity, you will use awk to make some changes to a file.

Instructions sent via Slack.

Suggested Time:
25 Minutes

Times Up! Let’s Review.

Start gAWK-ing

gAWK Review

Provide commands for the following solutions:

Print only the first field of the `17-18-Breaches.txt`.

Print only the breaches from 'web' companies.

Out of the web companies that were breached, print only the company names.

gAWK Review

Provide commands for the following solutions:

Print only the first field of the `17-18-Breaches.txt`.

```
awk -F"\t" '{print $1}' 17-18-Breaches.txt
```

Print only the breaches from 'web' companies.

Out of the web companies that were breached, print only the company names.

gAWK Review

Provide commands for the following solutions:

Print only the first field of the `17-18-Breaches.txt`.

```
awk -F"\t" '{print $1}' 17-18-Breaches.txt
```

Print only the breaches from 'web' companies.

```
awk '/web/' 17-18-Breaches.txt
```

Out of the web companies that were breached, print only the company names.

gAWK Review

Provide commands for the following solutions:

Print only the first field of the `17-18-Breaches.txt`.

```
awk -F"\t" '{print $1}' 17-18-Breaches.txt
```

Print only the breaches from 'web' companies.

```
awk '/web/' 17-18-Breaches.txt
```

Out of the web companies that were breached, print only the company names.

```
awk -F"\t" '/web/{print $1}' 17-18-Breaches.txt
```

gAWK Review

Provide commands for the following solutions:

Print all the breaches from 2017.

For the companies that had breaches in 2017, print only the company name and the number of records lost.

For the companies that had breaches in 2018, save the company name, company type and number of breaches to a new file named 2018Breaches.txt.

gAWK Review

Provide commands for the following solutions:

Print all the breaches from 2017.

```
awk '/2017/' 17-18-Breaches.txt
```

For the companies that had breaches in 2017, print only the company name and the number of records lost.

For the companies that had breaches in 2018, save the company name, company type and number of breaches to a new file named 2018Breaches.txt.

gAWK Review

Provide commands for the following solutions:

Print all the breaches from 2017.

```
awk '/2017/' 17-18-Breaches.txt
```

For the companies that had breaches in 2017, print only the company name and the number of records lost.

```
awk -F"\t" '/2017/{print $1, $3}' 17-18-Breaches.txt
```

For the companies that had breaches in 2018, save the company name, company type and number of breaches to a new file named 2018Breaches.txt.

gAWK Review

Provide commands for the following solutions:

Print all the breaches from 2017

```
awk '/2017/' 17-18-Breaches.txt
```

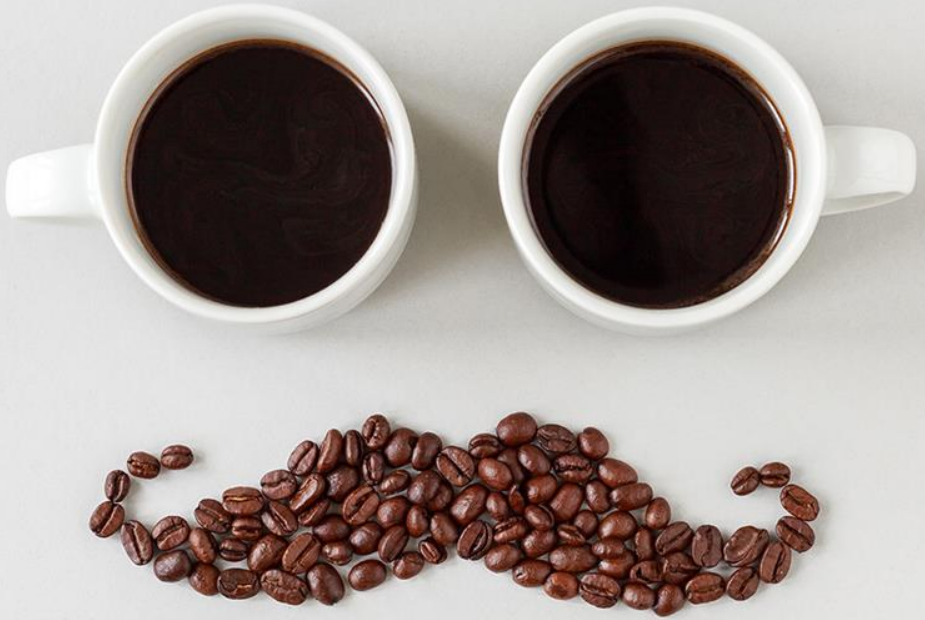
For the companies that had breaches in 2017, print only the company name and the number of records lost.

```
awk -F"\t" '/2017/{print $1, $3}' 17-18-Breaches.txt
```

For the companies that had breaches in 2018, save the company name, company type and number of breaches to a new file named 2018Breaches.txt.

```
awk -F"\t" '/2018/{print $1, $4, $3}' 17-18-Breaches.txt > 2018Breaches.txt
```

Take a Break!



Scavenger Hunt

Your Turn: Scavenger Hunt

In this next exercise, you will work in groups to find a series of "flags" on your Linux VM. Finding them will require the use of many Linux tools and concepts we've learned thus far, including:

- File permissions
- Command-line utilities like find
- Manipulating permissions with sudo and su

You will break up into groups of 4-5.

You should collaborate and share research amongst your group, but each student should perform each step on their own computer.

Times Up! Let’s Review.

Scavenger Hunt

Scavenger Hunt Review #1

Find an unusual-looking file in one of the `norse-guder` directories.

Hint #1: Find out which users are in the `norse-guder` group.

Hint #2: Use `find` to look for logs.

Scavenger Hunt Review #1

Find an unusual-looking file in one of the `norse-guder` directories.

Hint #1: Find out which users are in the `norse-guder` group.

Hint #2: Use `find` to look for logs.

Run `groups user` for each user on the system.

Run `find /home/ -iname '*.log'`

You should see a `webserver.log` in the home directory of the user Loki.

Scavenger Hunt Review #2

Use awk and/or sed to determine the distinct count of IP Addresses in the log file.

Hint: Use `awk` or `sed` to filter for IP addresses. Then pipe through other commands to remove duplicates. Finally, pipe to a command that counts lines.

Scavenger Hunt Review #2

Use awk and/or sed to determine the distinct count of IP Addresses in the log file.

Solution:

1. Use **head** to read the log file and note which column contains IP addresses.
2. Use this number in an awk command. E.g: `awk '{print $1}' webserver.log`
3. Next, pipe to **`sort`** and then `uniq`: `awk '{print $1}' webserver.log | sort | uniq`. This produces a list of only unique IP addresses.
4. Finally, pipe to `wc -l` to count lines: `awk '{print $1}' webserver.log | sort | uniq | wc -l`.

   You should count **51 IP addresses**.

Scavenger Hunt Review #3

Find the members of the **`hackers`** group and use the IP address count from the previous step as their password.

Scavenger Hunt Review #3

Find the members of the **`hackers`** group and use the IP address count from the previous step as their password.

- To find the members of the hackers group, you could run **`for i in $(ls /home); do groups $i; done | grep hacker`** or something similar.

- Or, just run `groups <user>` for each user listed in the home directory again.

- After trying 51 in various ways, you should be able to login to the user asgard using `fiftyone` for the password.

Scavenger Hunt Review #4

Login using the credentials found in the last step and look for a file with permissions: `-r--------` in that user's files. Make sure this file contains information about a person.

Hint: Use `ls` with special flags.

Scavenger Hunt Review #4

Login using the credentials found in the last step and look for a file with permissions: `-r---------` in that user's files. Make sure this file contains information about a person.

Hint: Use `ls` with special flags.

- There is a `contacts` directory in `~/asgard/contacts`.
- Move into that directory and use `ls -l`.
- You should see the permissions `-r---------` named `mickey.reichert`.
- Run `cat mickey.reichert` to reveal `hera iloveyou`.

Scavenger Hunt Review #4

Use the contents of the that file (re: last question) to log into this user’s account.

Hackers planted a file in the directory the kernel is stored in. Find it.

Scavenger Hunt Review #5

Use the contents of the file to log into this user's account.

Log into the account **`hera`** using the password **`iloveyou`**.

Hackers planted a file in the directory the kernel is stored in. Find it.

Scavenger Hunt Review #5

Use the contents of the file to log into this user's account.

Log into the account **`hera`** using the password **`iloveyou`**.

Hackers planted a file in the directory the kernel is stored in. Find it.

You should find the data file: **`/boot/blackhats.list`** .

Scavenger Hunt Review #6

Calculate the SHA 256 hash of the /boot/blackhats.list file.

Scavenger Hunt Review #6

Calculate the SHA 256 hash of the `/boot/blackhats.list` file.

- Run: **`sha256sum /boot/blackhats.list`**
- Should output:

  `97d054a8b3b6152e565a4e152f1db64a90cbbc5892c8809260148591b03559eb blackhats.list`

Submit the results of the above computation.

Any Questions?