Cybersecurity

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 on at least one task. Think of this as a relay race with each teammate helping out.

To complete this challenge, you will launch 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 TAs 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 remember them and you won't have to retrace any steps you've already completed.

Instructions

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

After logging into your web lab, complete the following:

- Open up the terminal.
- Run `sudo /home/sysadmin/Documents/scavenger-hunt/scavenger-hunt-start.sh`.
- Select option 1 to start the server for the first time.
- Allow the installation several minutes to take place.

After completing the install, you can log in via ssh by running:

- `ssh student@192.168.200.105`
- Then enter the following password: `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.

flag_2:

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

flag_3:

Find a `log` file related to the hacker's name and a `zip` file with additional info.

- 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.

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.

flag_5:

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

flag_6:

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

flag_7:

Find an exploit to gain a root shell. Log in as the root user.