**Exam/Quiz Module 3/Lesson 1 – CTF Linux Flags (INSTRUCTOR COPY)**

Date: Date

Points Possible: Suggested points for each question are indicated next to the question.

Please note that this assessment will only work with the K12 CYBER SECURITY CONCEPTS USING KALI LINUX on the Virginia Cyber Range. It will not work on any other Linux box. If a lab on the Virginia Cyber Range hasn’t been assigned to you, please check with your instructor.

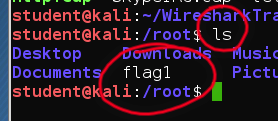
Question 1) FLAG 01: Simple flag (100pts)

There is a flag in the root's home directory (note this is /root and not the root directory (/)), you will know that it is a flag. (The answer is the file name of the flag).

Answer: flag1

Solution: (i) Go the home directory of the root (/root). Type the command ls.

Screenshot:



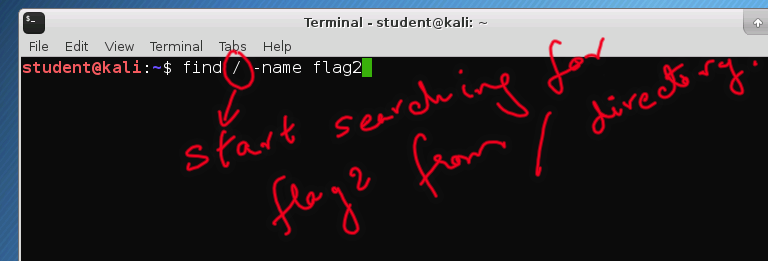
Question 2) FLAG 02: Find another flag and win big! (100pts)

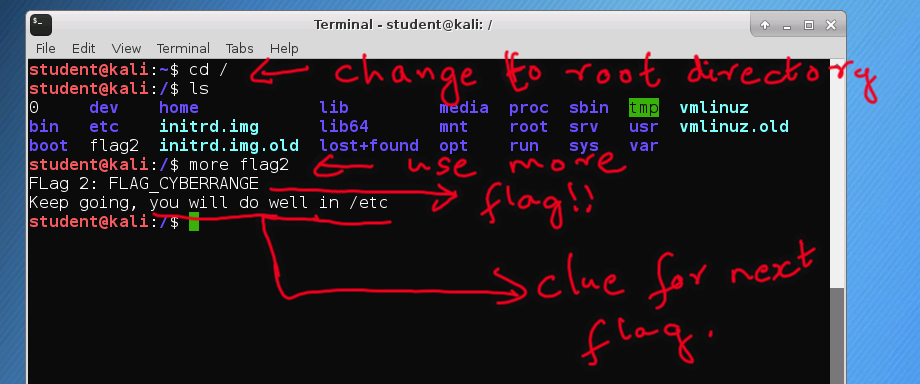
Find the flag inside the file flag2. The answer is the string that the flag asks you to enter.

Answer: FLAG\_CYBERRANGE

Solution: (i) Search for the flag from the root directory (/) using the command: find / -name flag2. (ii) Read the contents of the file (flag2 is in the root directory) using the more command: more flag2.

Screenshots:

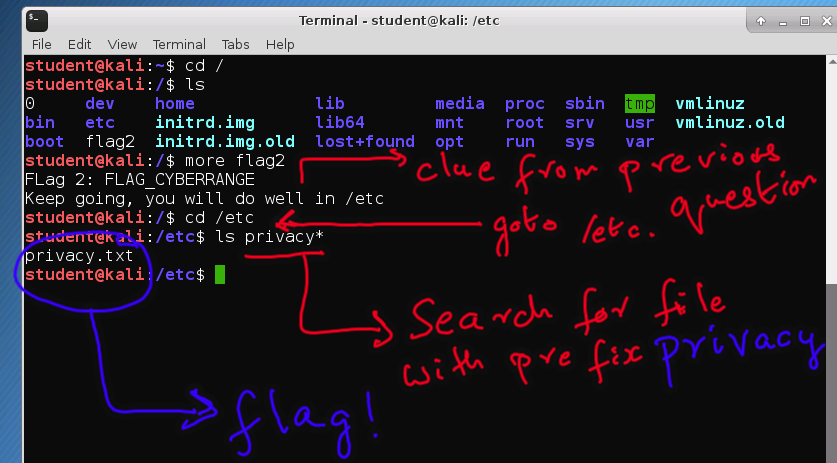




Question 3) FLAG 03: There is a private file that starts with the word privacy -- see the clue from FLAG 02 (Linux). What is the full name of the file? The answer is the entire filename including the extension, e.g., privacy.exe ).

Answer: privacy.txt

Screenshots



Question 4) FLAG 04: What does the private file say? (150pts)

The answer is the flag from the private file. You will know what the flag is when you find it.

Hint! Use grep.

Example: you can search for a text string (e.g., "flag"), inside a file (e.g., xyz.txt) this way:

more xyz.txt | grep "flag"

and yes! -- we used the vertical line which is above the back slash on the keyboard.

Answer: FLAG\_RANGE\_FOR\_PRIVACY

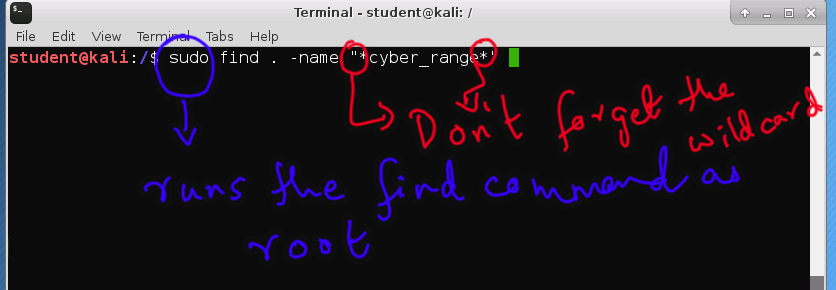
Question 5) FLAG 05: The range is the rage! (150pts)

How many filenames containing the word cyber\_range are on the Linux machine? The answer is a number.

Answer: 7

Solution: (i) For this question, running the find command as root user will avoid permission denied errors. (ii) The command: sudo find / -name “\*cyber\_range\*” will get you the answer. Please note that students may forget the wild card “\*” before and/or after the word “cyber\_range”. This wild card is important because the word cyber\_range may be any part of the file name.

Screenshots:



Question 6) FLAG 06: Who is this user? (150pts)

Identify the username of the user with user id = 0. Answer is just the username (one word).

Hint! Check the file: /etc/passwd. Here's how you can check (at the command prompt type):

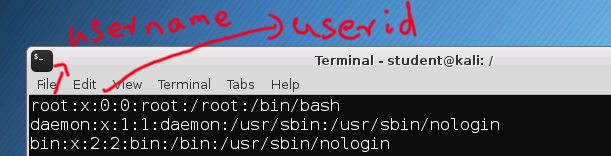
more /etc/passwd

Every line in this file corresponds to a user and is of the format:

username:x:userid:groupid:groupname:usershomedirectory:users\_shell.

Answer: root

Screenshots:



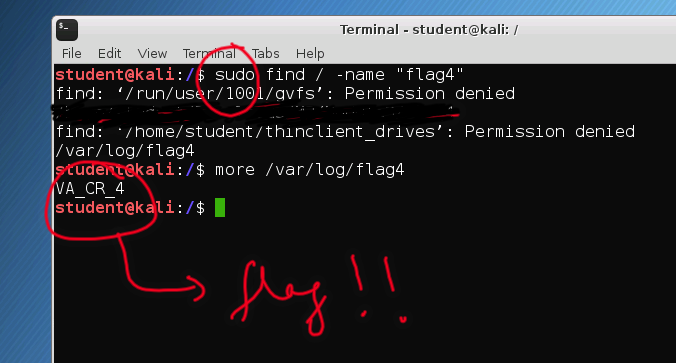
07 - Another flag! (150pts)

Find flag4 and enter the data inside it.

Answer: VA\_CR\_4

Solution: find / -name “flag4” then more /var/log/flag4

Screenshots:



08 - Hidden flags (200pts)

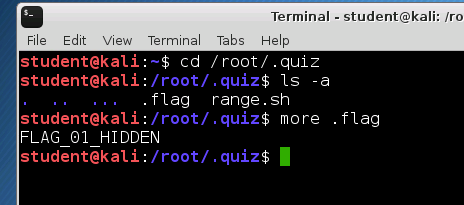
There is a file inside the directory: /root/.quiz. Find the flag inside the file. Note, the file may be hidden. Flag format is: FLAG-XY-ABCD (e.g., FLAG\_ID\_12$\*).

Hint! In Linux, hidden files start with the dot ".". E.g., .quiz is a hidden directory. To find all hidden files and directories, run: "ls -al \*" in the appropriate directory. E.g., to find the hidden file in the /root/.quiz directory, here are the steps: (1) cd /root/.quiz; (2) ls –a

To reveal the contents of a file, remember to use the "more" command.

Answer: FLAG\_01\_HIDDEN

Screenshots:



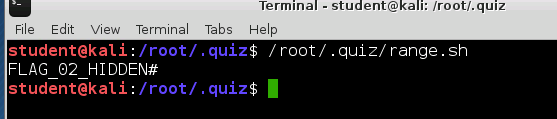
09 - Run this program and get a flag. (200pts)

Go to the hidden folder and run the range.sh program to get the flag. Flag format: FLAG-XY-ABCD

Hint! To execute a program, use the absolute pathname of the program.

(1) Type: cd /root/.quiz (2) Type: /root/.quiz/range.sh

Answer: FLAG\_02\_HIDDEN#



10 - All on your own! (250pts)

Flag based on a file named range2.sh. Find it.

Answer: RANGE\_IS\_THE\_RAGE

Solutions: (i) sudo find / -name “range2.sh” ; (ii) Run the code: /root/.quiz/.../range2.sh. The file range2.sh is hidden in a hidden directory called “…”. Run that code.

[This portion of the exams/quizzes template is provided for instructors that will be using this exam/quiz in a class they are teaching.]

This assessment provides students with hands on experience on the Linux machine provided on the cyber range along with this course. To work on the assessment:

1. Students must login to the Linux machine with username and password provided on the range.
2. Start a terminal on the Linux machine.
3. Use the command line interface (CLI) on the terminal to search for flags. A flag is a filename or some string inside a file.
4. 01\_Linux\_ASSESSMENT\_INSTRUCTORCOPY.docx provides hints, solutions and answers for all the questions in the assessment.