Sudo Misconfiguration Report - 22.5.1 - 22

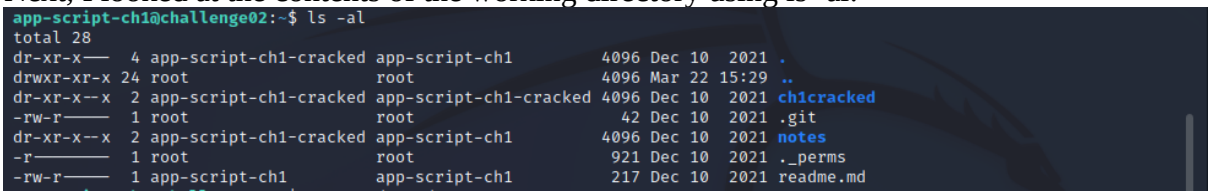
Tester's name: Stanley Ford

Lab №22.5.1 "Sudo Misconfiguration" :

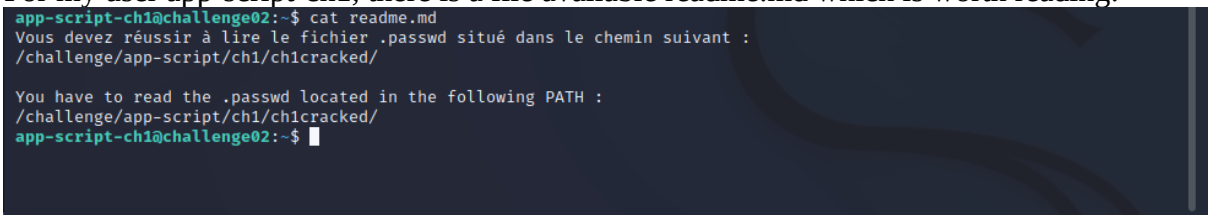
- General information:
  - Testing period: 01.04.2023
  - Test object: challenge02.root-me.org
- Description of actions:

  When I connected to the ssh server, the first thing I did was check the id, whoami, uname -a commands to understand what I was working with.

  Next, I looked at the contents of the working directory using ls -al:

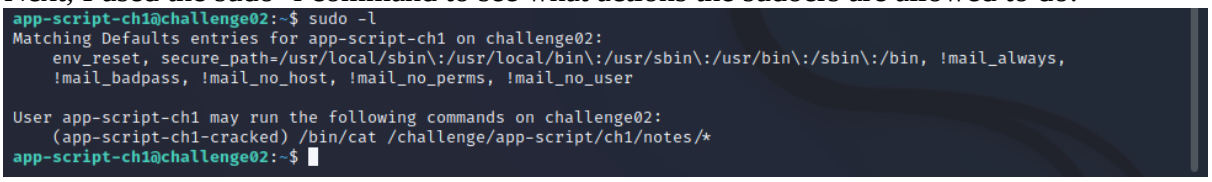


  For my user app-script-ch1, there is a file available readme.md which is worth reading:



  Thus, the flag you are looking for lies in .passwd along the above path.

Next, I used the sudo -l command to see what actions the sudoers are allowed to do:

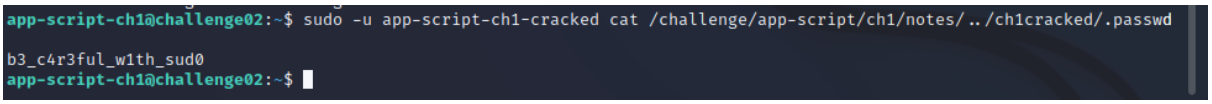


Thus, with sudo, we can only run the command /bin/cat /challenge/app-script/ch1/notes/* on behalf of our user.

* At the end of the path, there is a weak point. This symbol means that you can substitute anything for it and execute any command, as long as the part of the path to it coincides. That is, you can run the command:

sudo -u app-script-ch1-cracked cat /challenge/appscript/ch1/notes/.. /ch1cracked/.passwd

It will run the /bin/cat binary as app-script-cracked and read the file at /.. /notes, will go up one directory ".. /" and will go to ch1cracked/.passwd, where the flag is:



Flag:

b3_c4r3ful_w1th_sud0

Lab work is done.

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab:

  Kali Linux terminal

- List the vulnerabilities you've discovered:

  Sudo Misconfiguration

- Give advice on how to improve protection:

  Specify the specific path of the allowed commands so that it is not possible to exploit them by jumping up the directory.