The find command - Tryhackme

I. Overview

Use to search for files in a directory hierarchy

Syntax: find where what

- where: specify the directory where to look
- what : specify what to look for

II. Usage

1. Decentralization.

r: read - 100
w: write - 010
x: execute - 001
-: deny - 000

2. Some common Flag :

- -type: specify type of target
  - d : directory
  - f : file
- -name: specify a name or pattern (-name abc.xyz)
  - If use wildcards, need to enclose your pattern in quotes ("*.xyz")
- -iname: use the same as –name , but case insensitive
- -user: specify username of owner of file. (-user s0vvn –name vl.txt)
- -size: specify size of a file.
  - **Prefix**: "- ", "+",
    - -n : size < n
    - +n : size >n
    - n : size =n
  - **Suffix:**
    - c: bytes
    - k: KB
    - m: MB
- -perm: specify permission

  Prefix :

  - "-": return files with **at least** the permissions you specify.
  - "/": return files that match **any** of the permissions you have set
- **time-related:** e.g: -amin –30 (find file was accessed < 30' ago)
  - min: minutes
  - time: days
  - a: accessed

- m: modified
- c: changed
- +,-,””: Use the same as size

III. Practice

1. Find all files owned by the user "kittycat":

- All file => directory = / & –type f & ‘-user kittycat’

Find all files owned by the user "kittycat"

find / -type f -user kittycat

Correct Answer

2. Find all files that are exactly 150 bytes in size

- Directory: / & -type f & -size 150c

Find all files that are exactly 150 bytes in size

find / -type f -size 150c

Correct Answer

3. Find all files in the /home directory (recursive) with size less than 2 KiB’s and extension ".txt"

- Directory: /home & -type f & -size –2k && -name “*.txt”

Find all files in the /home directory (recursive) with size less than 2 KiB's and extension ".txt"

find /home -type f -size -2k -name "*.txt"

Correct Answer

4. Find all files that are exactly readable and writeable by the owner, and readable by everyone else (use octal format)

- Directory: / &-type f & -perm (owner:6, g:4 ,other:4) 644

Find all files that are exactly readable and writeable by the owner, and readable by everyone else (use octal format)

find / -type f -perm 644

Correct Answer

5. Find all files that are **only** readable by anyone (use octal format)

- Dir: / & -type f & -perm /444

Find all files that are **only** readable by anyone (use octal format)

find / -type f -perm /444

Correct Answer

6. Find all files with write permission for the group "others", regardless of any other permissions, with extension ".sh" (use symbolic format)

- Dir: / & -type f & -perm -o=w & -name “*.sh”

Find all files with write permission for the group "others", regardless of any other permissions, with extension ".sh" (use symbolic format)

find / -type f -perm -o=w -name "*.sh"

Correct Answer

7. Find all files in the /usr/bin directory (recursive) that are owned by root and have at least the SUID permission (use symbolic format)

- Dir: /usr/bin & -type f & -user root & -perm –u=s(s: execute file as permission of owner)

Find all files in the /usr/bin directory (recursive) that are owned by root and have at least the SUID permission (use symbolic format)

find /usr/bin -type f -user root -perm -u=s

Correct Answer

8. Find all files that were not accessed in the last 10 days with extension ".png"

- Dir: / & -type f & -atime –10 & -name “*.png”

Find all files that were not accessed in the last 10 days with extension ".png"

find / -type f -atime +10 -name "*.png"

Correct Answer

9. Find all files in the /usr/bin directory (recursive) that have been modified within the last 2 hours
- Dir: /usr/bin & -type f & -mmin –120.

Find all files in the /usr/bin directory (recursive) that have been modified within the last 2 hours

find /usr/bin -type f -mmin -120

Correct Answer