NASA hw0 System Administration

Student

- Name: 林楷恩
- ID: B07902075

1. Welcome abroad!

- `$ ssh b07902075@nasa-hw0.csie.ntu.edu.tw`

2. The Oracle

- `$ man Pittheus`

3. Know thy place

- `$ pwd`

4. Sandals and Swords

- `$ cd ~/ship/Theseus's_Room`
- `$ chmod u+w big_rock .` # to get the permission of changing the content of the directories
- `$ mv big_rock/sandals* big_rock/sword* .`
- `$ rm -r big_rock`
- `$ ./Aegeus`

5. Hargghh MATE!

- `$ cd ~/ship/master_room`
- `$ ls -a` # to see the hidden files
- `$ cat .captain`

6. Sinking ship

- `$ cat ./SINKING_SHIP | sed 's/bugs//gI' | grep 'NASA{.\{1,100\}}' -o`
- **ref.**
    1. https://www.cyberciti.biz/faq/unixlinux-sed-case-insensitive-search-replace-matching/

7. Handy man

- `$ cd ~/ship/master_room`
- `$ sort KEY | uniq -u` # get the key
- `$ chmod u+w .` # to create file in this directory
- `$ unzip tool_box.zip` # use the key to unzip file
- `$ cat tool_box/tool.txt`
- **ref.**
    1. `man uniq`
    2. `man unzip`

8. King of the Labyrinth

- First create another panel with `tmux`

- Run `beast` in one of the panel
- Switch to another panel
- `$ ps a` # Find out the `PID` of `beast` process
- `$ kill -15 PID` # send a `SIGTERM` signal to it
- **ref.**
    1. https://superuser.com/questions/243460/what-to-do-when-ctrl-c-cant-kill-a-process
    2. `man kill`

9. Voyage back

- `$ find / -name 'white_mast' 2> /dev/null`
- `$ cat /opt/white_mast`
- **ref.**
    1. `man find`

10. Ship of Theseus

- Read pong_game.py and find that something is listening on port 10101, which is sending the logo.

  ```
  r = remote('127.0.0.1', 10101)
  r.sendlineafter('mode:\n',mode)
  data = r.recv()[:-1]
  r.close()
  ```

- And I summary that the process behind it first receives "mode" which is default "Theseus" in pong_game.py, then sends the logo to us. I can also deduce that there are still some message in it since it use `sendlineafter()` method which expect a prompt message ('mode:\n') before sending the mode. Thus, I use `r.interactive()` to view the whole process transparently.

- (In python3 shell)

  ```
  >>> r = remote('127.0.0.1', 10101)
  >>> r.interactive()
  ```

- ...then get the tip informing me to find logo2

- `$ find / -name 'logo2' 2> /dev/null`

- Find `/mnt/nasa/logo2` and other files in the same directory

- Based on "Theseus is special", I make a guess that only "Theseus" mode leads to additional operations which get the original logo.

- Furthermore, the 3 found files are readable only for root, so I must read it through root's operation. The obvious way(or maybe the only option given that the only operation we can do is sending it a mode) to do this is to provide the root the absolute path of them. Thus, I then try to "replace" `mode` with the path of these files. The tip from the end of Pittheus's secret more or less help here.

- Finally, find the flag in `/mnt/nasa/Zeus`

- P.S. In the output of `$ ps a`, we can view the parameters of the listening process "`ncat -vc python2 pong.py -kl 10101 -o nclog`", so we can combine it with the previous discovery to see the source code by replace mode with pong.py.

- **ref.**
    1. http://docs.pwntools.com/en/stable/
    2. `man ncat`

3. https://www.devglan.com/online-tools/aes-encryption-decryption (for decrypt Pittheus's secret)
4. https://www.base64decode.org/ (for decrypt Pittheus's secret)