PONDERING PATHS

The PATH Variable

`/challenge/run` deletes the flag using `rm`. This can be avoided by just remvoing access to `rm`. `PATH=""` empties the PATH variable and now `rm` can no longer be accessed

flag-`pwn.college{E238k985E9kXkEvp0eeUsc7QkFR.dZzNwUDL3YjN0czW}`

Setting PATH

`/challenge/run` invokes `win` with it's bare name. Since `win` is in the `/challenge/more_commands/` directory, we need to add that to PATH.

`PATH="/challenge/more_commands/"`

Now running `/challenge/run`, gives the flag:`pwn.college{8RO0SnWJ5C-ZNogBM1HTaAUqugm.dVzNyUDL3YjN0czW}`

Adding Commands

So this challenge involves the following processes: create a shell script called `win` which gets the flag, set the PATH variable properly to access both `win` and whatever command required to retrieve flag(in this case `cat`) and then finally run `/challenge/run`

I created a folder called `windir` to have the `win` script in the home directory using `mkdir windir` Then I used `cd windir` and then `touch win` to create the script Edited the script using `nano` and added `cat /flag` to the file

Now I needed to figure out which folder `cat` was saved in so I could make sure to let it remain in the PATH variable

`echo $PATH` gives the output

```
/run/challenge/bin:/run/workspace/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

```

```
hacker@path~adding-commands:~$ cd ~
hacker@path~adding-commands:~$ $flga
hacker@path~adding-commands:~$ $flag
hacker@path~adding-commands:~$ nano win
hacker@path~adding-commands:~$ chmod +x win
hacker@path~adding-commands:~$ PATH=/home/hacker
hacker@path~adding-commands:~$ /challenge/run
Invoking 'win'....
pwn.college{cU1H6Ab-o-OlMql0v3HzawIb9EM.dZzNyUDL3YjN0czW}
```

Hijacking Commands

In this module you need stop `/challenge/run` from deleting the flag by using `rm` and also print the flag.

My first idea was to create a script called `rm` that is basically a copy of `win` from the previous challenge and put the locations of only the new `rm` and `cat` in PATH. The thing I didn't consider is that `rm` is in the same directory as `cat`.

```
hacker@path~hijacking-commands:~$ cd ~
hacker@path~hijacking-commands:~$ $flag
hacker@path~hijacking-commands:~$ nano rm
hacker@path~hijacking-commands:~$ chmod +x rm
hacker@path~hijacking-commands:~$ PATH=/home/hacker
hacker@path~hijacking-commands:~$ /challenge/run
Trying to remove /flag...
pwn.college{kLT9aI1soyIjKUpp23plfOQbuAS.ddzNyUDL3YjN0czW}
```