# Unix security hole

➡ Even without root (or setuid)
attackers can trick root owned processes into doing things

Example - clear unused files in /tmp every night

```
$ find /tmp -atime +3 -exec rm -f -- {} \;
```

- `find` identifies files not accessed in 3 days
- rm -f -- path deletes file path

# Let us look at the system calls

| find/rm | Attacker |
| --- | --- |
| | mkdir (“/tmp/badetc”) |
| | creat (“/tmp/badetc/passwd”) |
| readdir (“/tmp”) → “badetc” | |
| lstat (“/tmp/badetc”) → DIRECTORY | |
| readdir (“/tmp/badetc”) → “passwd” | |
| unlink (“/tmp/badetc/passwd”) | |