Hiding from `ls`

Learning Objectives

- Design and implement a C program using structured programming techniques
- Design and implement a C program applying secure cyber design
- Design and implement a C program that initially creates a file on disk using Descriptor I/O, but then removes the file from the physical disk while still utilizing the file resident in memory
- Design and implement a C program that uses Descriptor I/O to change the name of a file on disk, where the file to change names will be specified via a command line argument

Before Class

In preparation for in class activities, complete the following activities:

- None.

In Class

Assignment Information

in operations: Temp Directories On UNIX systems the `/tmp/` directory is world readable and world writeable. Processes often use the `/tmp/` directory as a scratch space. The common practice in UNIX is for temp directories to be accessible only via the local system, i.e. temp directories are not mounted remotely across the network. This makes temp directories good places for malware to reside on disk; it takes extra steps for operators to keep track of what is in the temp directories on systems. OSes vs. Temp Directories:

- UNIX: `/tmp/` (non-persistent across reboots), `/var/tmp/` (persistent across reboots)
- Windows Early era: `C:\Temp\`
- Windows XP era: `[user]\Local Settings\Temp\`
- Windows 7 era: `[user]\AppData\Local\Temp\`

in the news: BlackPOS Anti-Forensics In the Fall of 2013 Target was breached by malware that specifically targeted the Point-of-Sale (POS) register software that handled customer credit card information. BlackPOS used anti-forensics techniques that included the malware deleting itself from systems that did not have the Point-of-Sale software that the malware was targeting.

Lab 0x02: Hiding from `ls`

Assignment Type:	Programming - Laboratory	Collaboration Policy:	Default
Assignment		Lab 0x02: Hiding from `ls`	
Due			

Section	Course Server Time / Date
1121	Pseudo Code: Friday, 1800 24 Feb 2018 Complete: Tuesday, 0755 28 Feb 2018
3122	Pseudo Code: Friday, 1800 24 Feb 2018 Complete: Tuesday, 0955 28 Feb 2018
5123	Pseudo Code: Friday, 1800 24 Feb 2018 Complete: Tuesday, 1330 28 Feb 2018

General Comments:

- Make use of in-class time to the fullest extent possible
- Read the entire assignment before you begin
- You are given more time to complete programming assignments because they are expected to take you longer to complete
    - It is expected that you will need to work on programming assignments outside of scheduled class
    - Do not procrastinate on starting a programming assignment

Given Material:

- Starter Code: `lsHiding.c`
- Test Script: `run-test.sh`
- Compiled Solution: `lsHiding` (x86-64)
  SHA-256: `845f0624a27ba6acac2cc67489ca8443205cff6d7a3ebe7b4908d9e391583762`

Test

The following are examples of how your program may be tested from the command line.

```
$ pwd
/tmp

$ ./lsHiding file1.xxx  # Part 1
Pause Point: File appears in ls listing
^Z
[1]+ Stopped        ./lsHiding
$ ls -i
...
2020 file1.xxx
...
$ fg 1
./lsHiding
8
Pause Point: File does not appear in ls listing, but still open
^Z
[1]+ Stopped        ./lsHiding
$ ls -i
...
...
$ fg 1
./lsHiding
8
$ echo $?
0
$

$ ./lsHiding lsHiding  # Part 2
Pause Point: File appears in ls listing
^Z
[1]+ Stopped        ./lsHiding
```

```
$ ls -i
...
2020 lsHiding
...
$ fg 1
./lsHiding
8
Pause Point: File does not appear in ls listing, but still open
^Z
[1]+ Stopped        ./lsHiding
$ ls -i
...
...
$ fg 1
./lsHiding
8
$ echo $?
0
$ ls -li
...
2021 -rwx------ m2O#### mids 1 #### Mmm dd hh:mm hide-H4XOrd
...
$

$ ./lsHiding fileDNE.bad  # Error
lsHiding-ERROR 1-fileDNE.bad: No such file or directory
$ echo $?
1
$
```

After Class

Activities

Furthering the in class activities, complete the following activities:

in the news: Fileless Malware In Feb 2017 *Kaspersky Labs* reported about cyber operations targeting enterprises that relied on *fileless* malware to deter detetection by cyber hunt teams. That is the malware only existed in RAM, there were no files within the filesystem, no files were written to disk my the malware. The report, and other articles (*Kaspersky Lab, U.S.*, *Cyber Scoop*) summarize some of the other methods employed in the operations and the overall campaign(s).

- Turn in the worksheet to your instructor after you have submitted your final source code.
- Submit your pseudo code in a single file named `lsHidingPseudo.c`, following the submission directions on the course information web page.
- Submit your final source code in a single file named `lsHiding-#.c`, where `#` is the part of the implementation that you completed (e.g. `lsHiding-2.c`), following the submission directions on the course information web page.

`submit` Assignment (project): *lab02*

Resources

Assignment Solutions:

- Worksheet Solution: Hiding from `ls`
- Source Code Solution: lsHiding.c
  SHA-256: `f05213b374f86212256593c8560ac0061316b7cf110ee2ac8e8cca28286fa012`