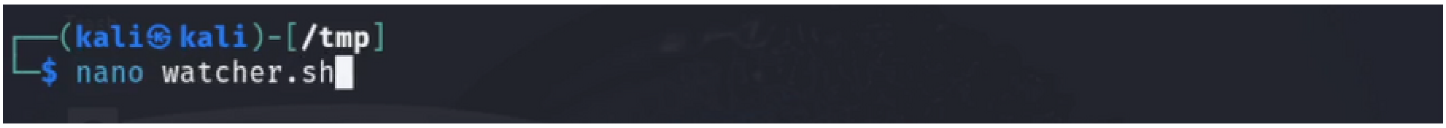
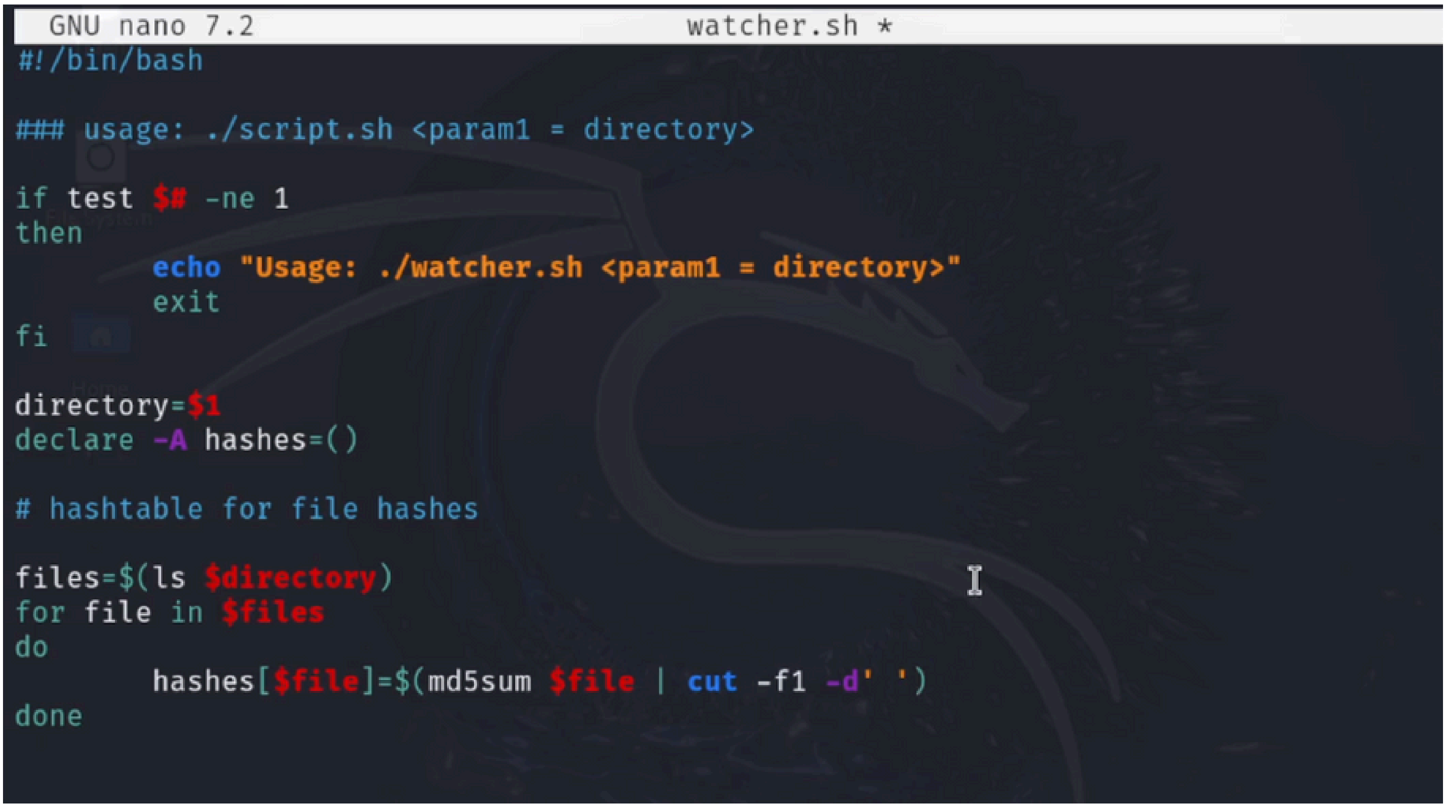
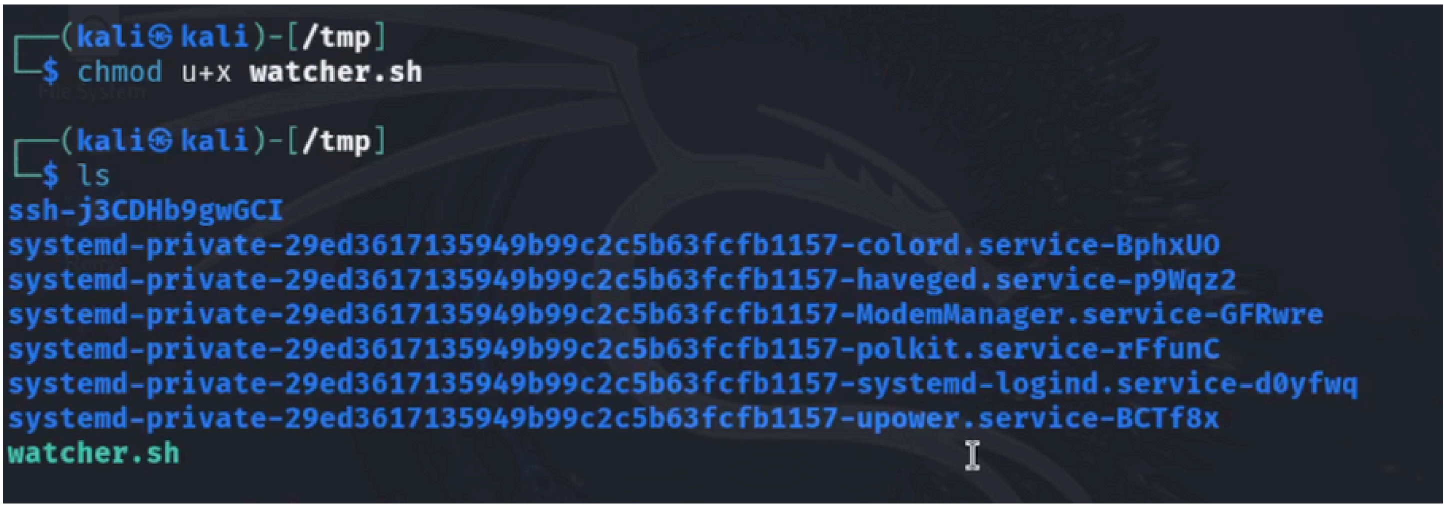


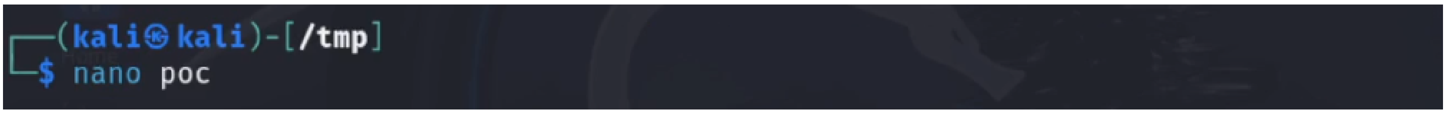
```
┌──(kali㉿kali)-[/tmp]
└─$ nano watcher.sh
```



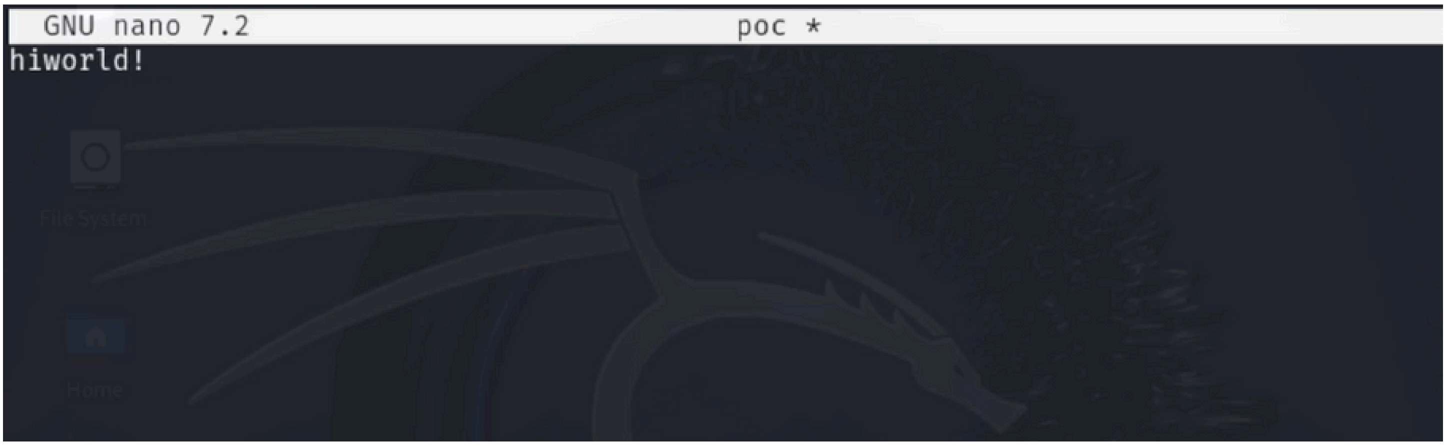
```
 GNU nano 7.2                              watcher.sh *
#!/bin/bash

### usage: ./script.sh <param1 = directory>

if test $# -ne 1
then
        echo "Usage: ./watcher.sh <param1 = directory>"
        exit
fi

directory=$1
declare -A hashes=()

# hashtable for file hashes

files=$(ls $directory)
for file in $files
do
        hashes[$file]=$(md5sum $file | cut -f1 -d' ')
done
```



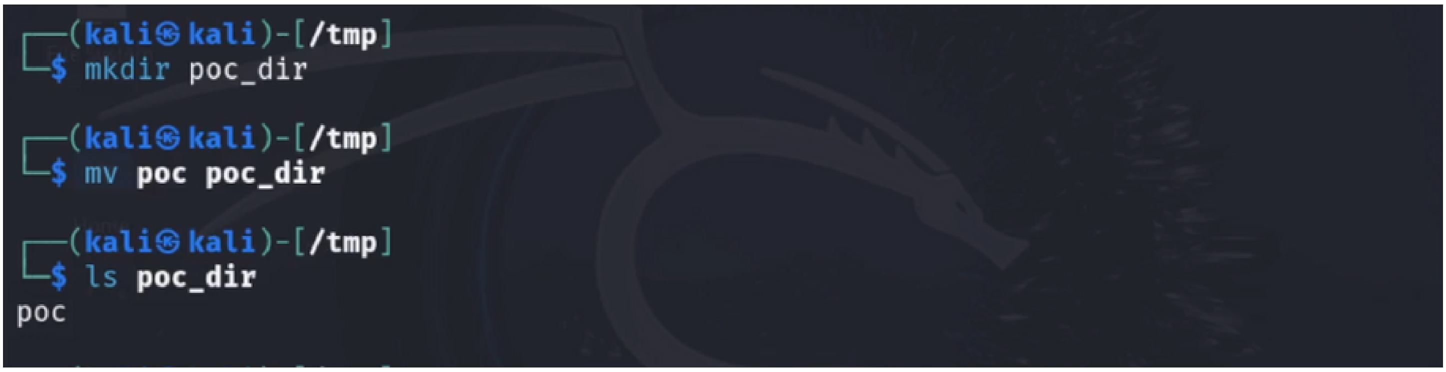
```
┌──(kali㉿kali)-[/tmp]
└─$ chmod u+x watcher.sh

┌──(kali㉿kali)-[/tmp]
└─$ ls
ssh-j3CDHb9gwGCI
systemd-private-29ed3617135949b99c2c5b63fcfb1157-colord.service-BphxUO
systemd-private-29ed3617135949b99c2c5b63fcfb1157-haveged.service-p9Wqz2
systemd-private-29ed3617135949b99c2c5b63fcfb1157-ModemManager.service-GFRwre
systemd-private-29ed3617135949b99c2c5b63fcfb1157-polkit.service-rFfunC
systemd-private-29ed3617135949b99c2c5b63fcfb1157-systemd-logind.service-d0yfwq
systemd-private-29ed3617135949b99c2c5b63fcfb1157-upower.service-BCTf8x
watcher.sh
```



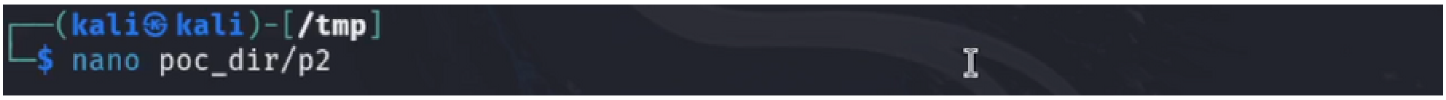
```
┌──(kali㉿kali)-[/tmp]
└─$ nano poc
```



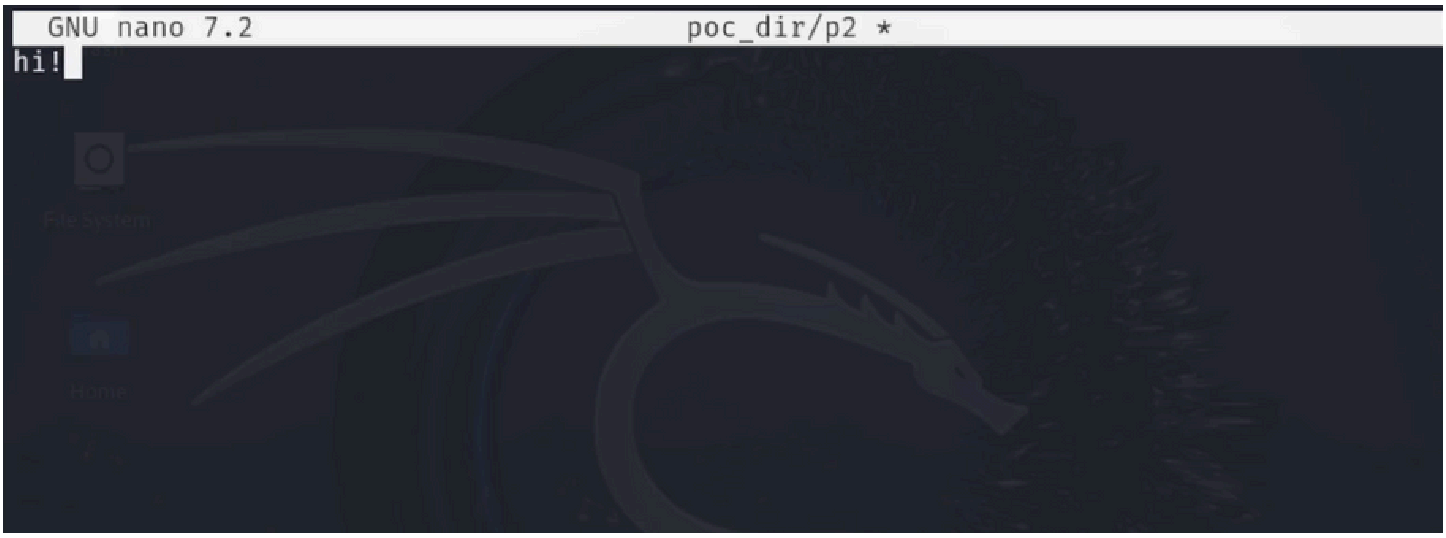
```
 GNU nano 7.2                              poc *
hiworld!
```



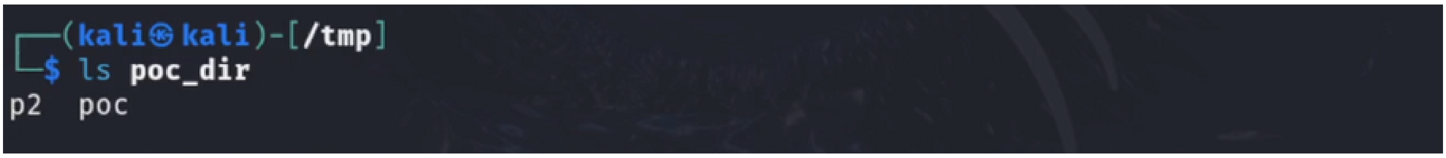
```
┌──(kali㉿kali)-[/tmp]
└─$ mkdir poc_dir

┌──(kali㉿kali)-[/tmp]
└─$ mv poc poc_dir

┌──(kali㉿kali)-[/tmp]
└─$ ls poc_dir
poc
```



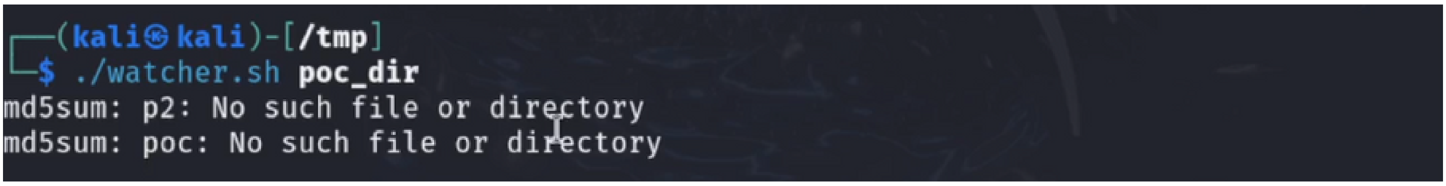
```
┌──(kali㉿kali)-[/tmp]
└─$ nano poc_dir/p2
```



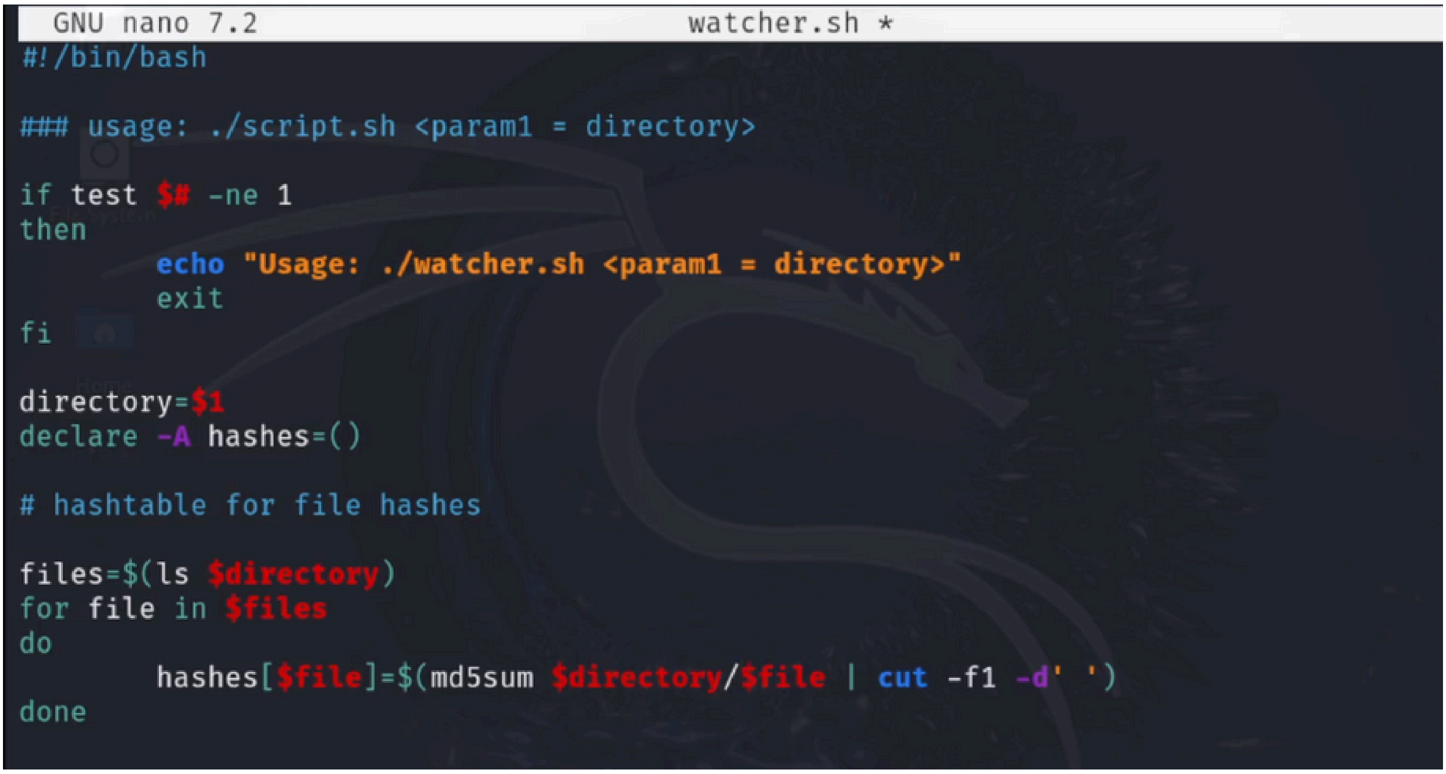
```
  GNU nano 7.2                     poc_dir/p2 *
hi!
```



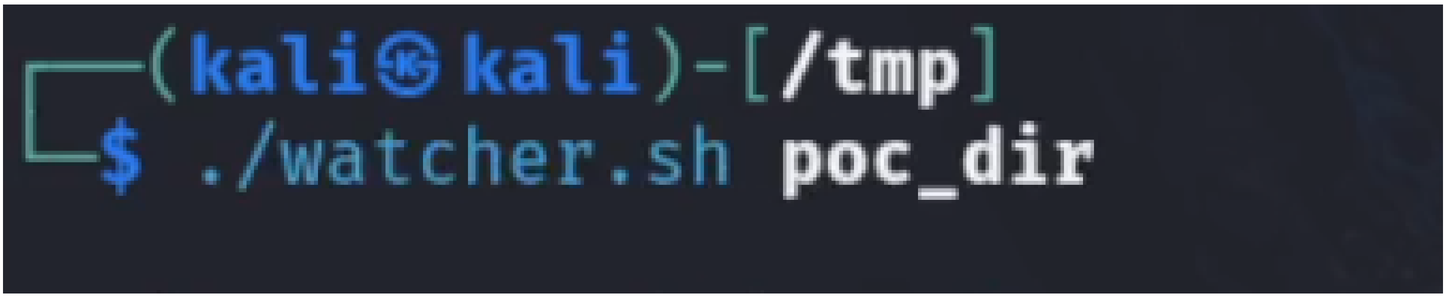
```
┌──(kali㉿kali)-[/tmp]
└─$ ls poc_dir
p2  poc
```



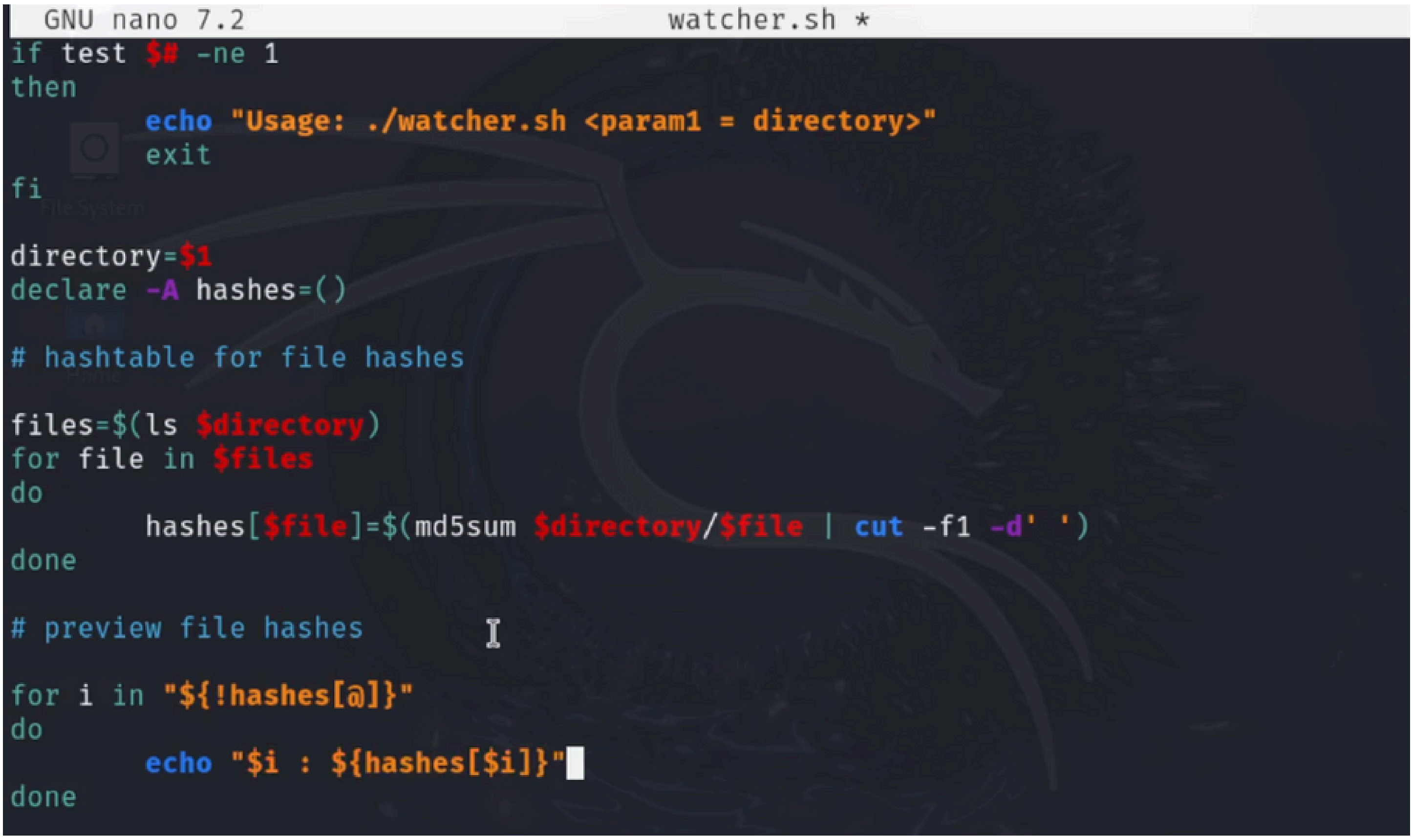
```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
md5sum: p2: No such file or directory
md5sum: poc: No such file or directory
```



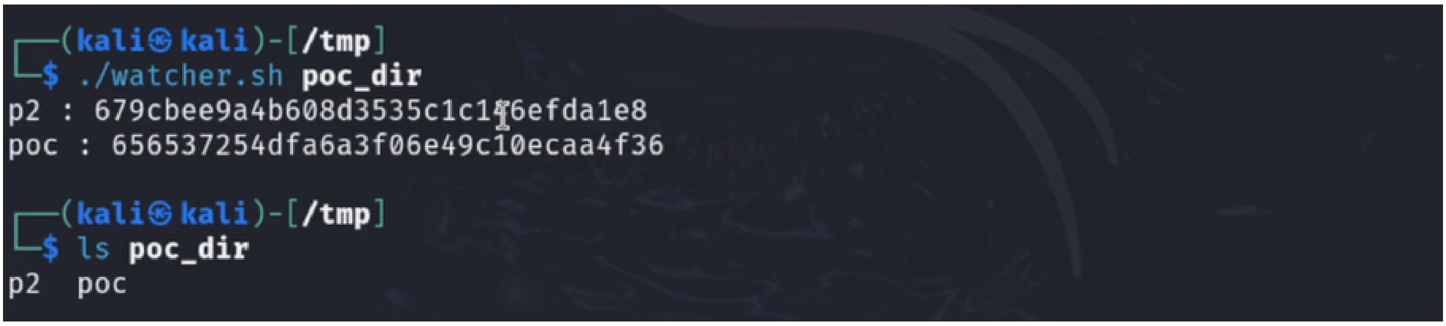
```
#!/bin/bash

### usage: ./script.sh <param1 = directory>

if test $# -ne 1
then
        echo "Usage: ./watcher.sh <param1 = directory>"
        exit
fi

directory=$1
declare -A hashes=()

# hashtable for file hashes

files=$(ls $directory)
for file in $files
do
        hashes[$file]=$(md5sum $directory/$file | cut -f1 -d' ')
done
```



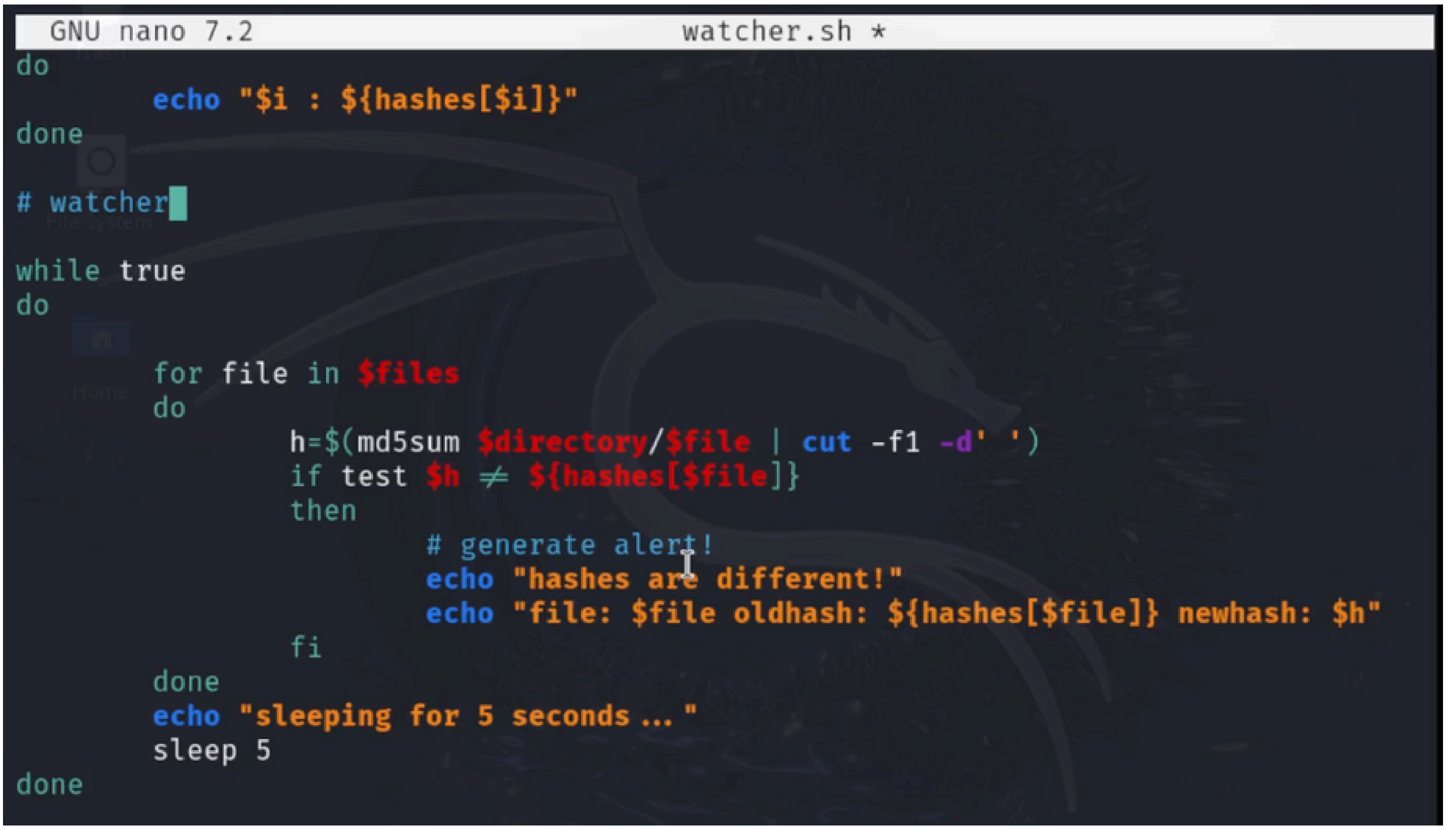
```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
```



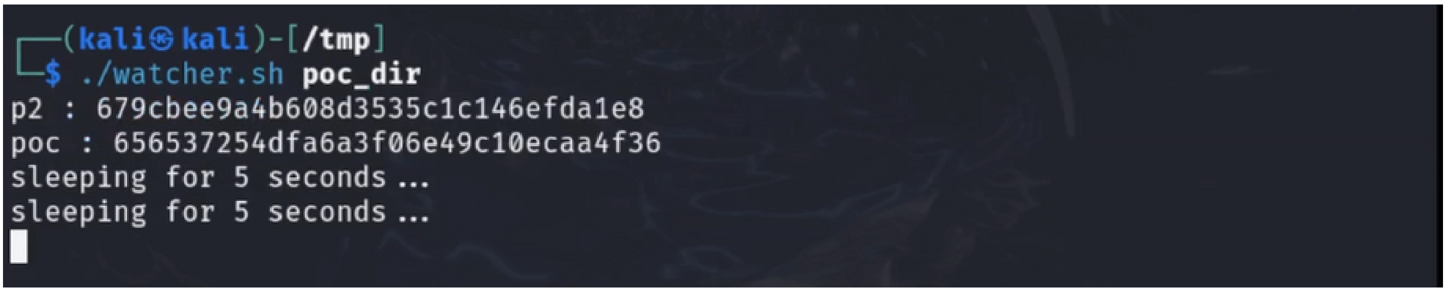
```
if test $# -ne 1
then
        echo "Usage: ./watcher.sh <param1 = directory>"
        exit
fi

directory=$1
declare -A hashes=()

# hashtable for file hashes

files=$(ls $directory)
for file in $files
do
        hashes[$file]=$(md5sum $directory/$file | cut -f1 -d' ')
done

# preview file hashes

for i in "${!hashes[@]}"
do
        echo "$i : ${hashes[$i]}"
done
```



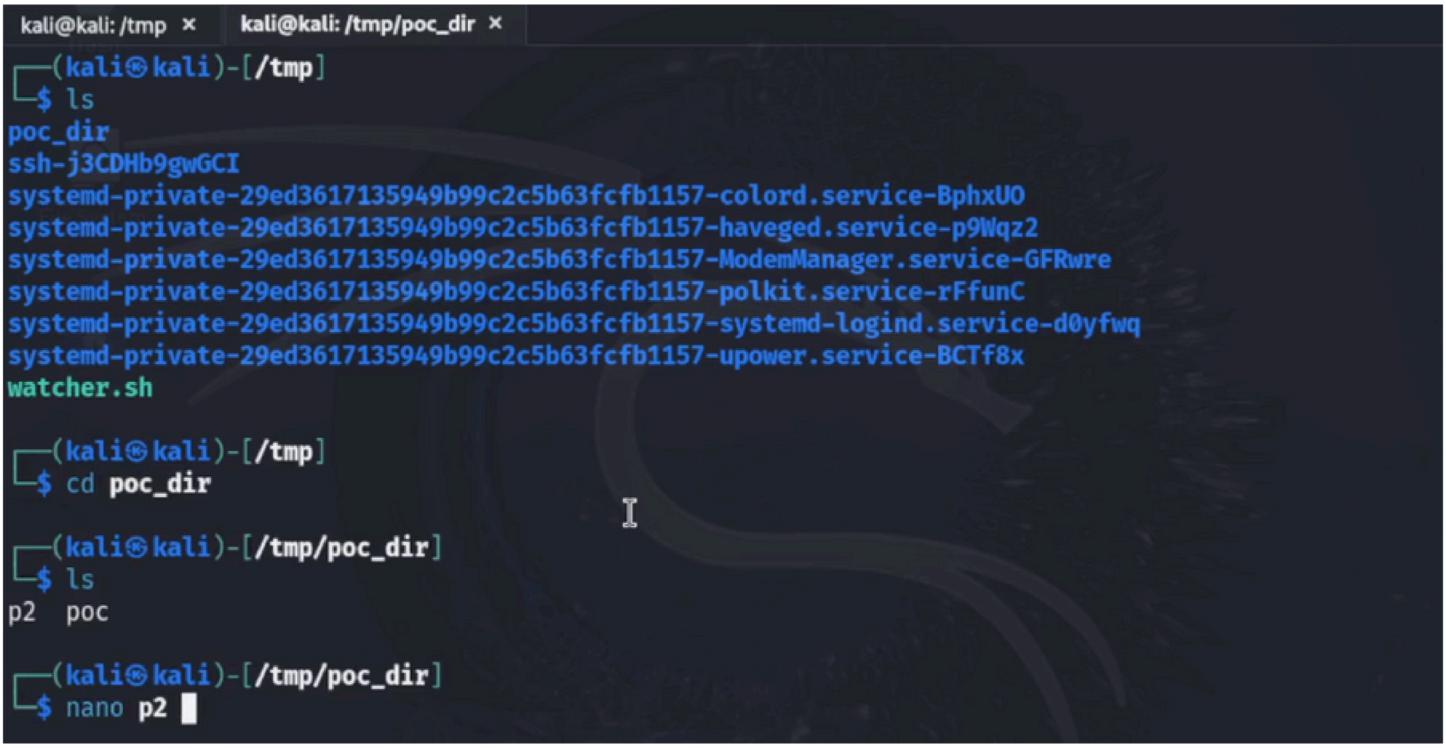
```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
p2 : 679cbee9a4b608d3535c1c146efda1e8
poc : 656537254dfa6a3f06e49c10ecaa4f36

┌──(kali㉿kali)-[/tmp]
└─$ ls poc_dir
p2  poc
```



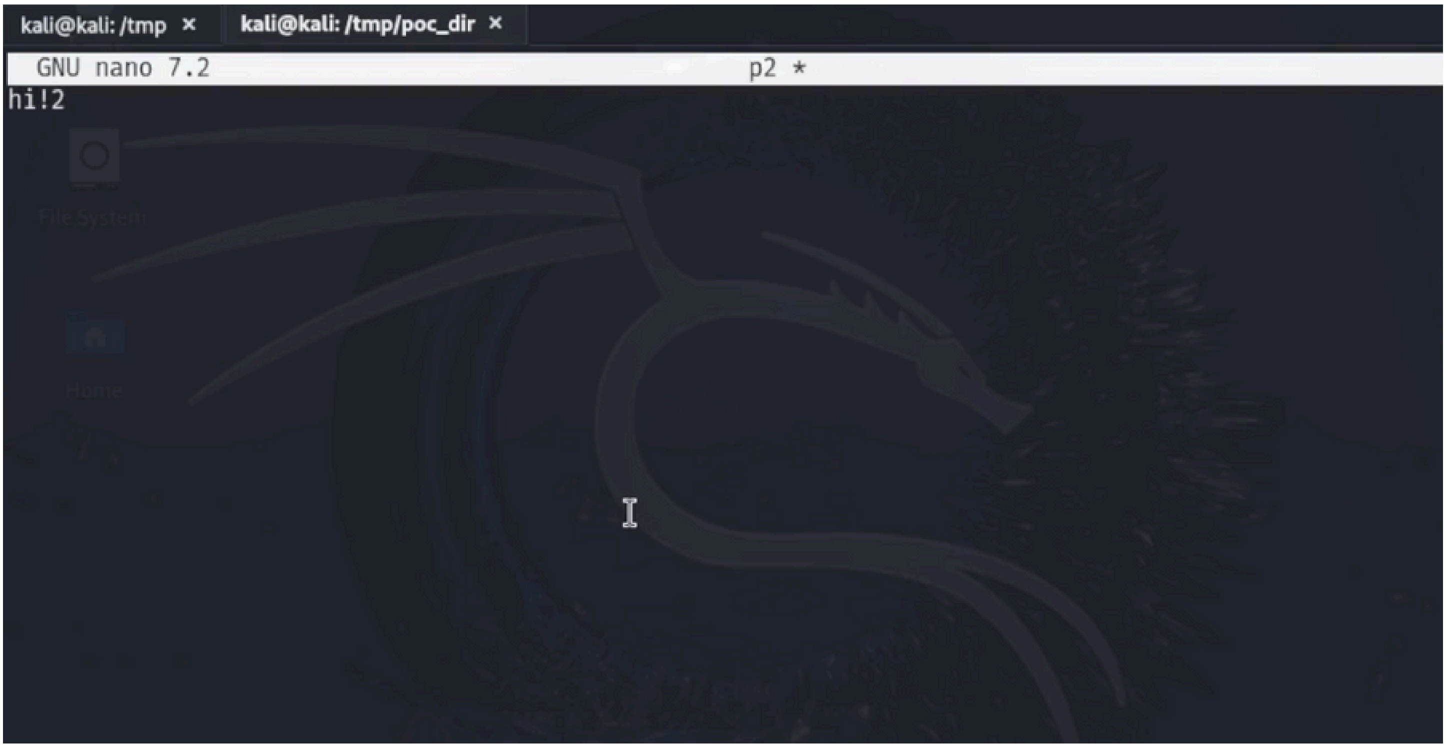
```
 GNU nano 7.2                          watcher.sh *
do
        echo "$i : ${hashes[$i]}"
done

# watcher

while true
do

        for file in $files
        do
                h=$(md5sum $directory/$file | cut -f1 -d' ')
                if test $h ≠ ${hashes[$file]}
                then
                        # generate alert!
                        echo "hashes are different!"
                        echo "file: $file oldhash: ${hashes[$file]} newhash: $h"
                fi
        done
        echo "sleeping for 5 seconds ... "
        sleep 5
done
```



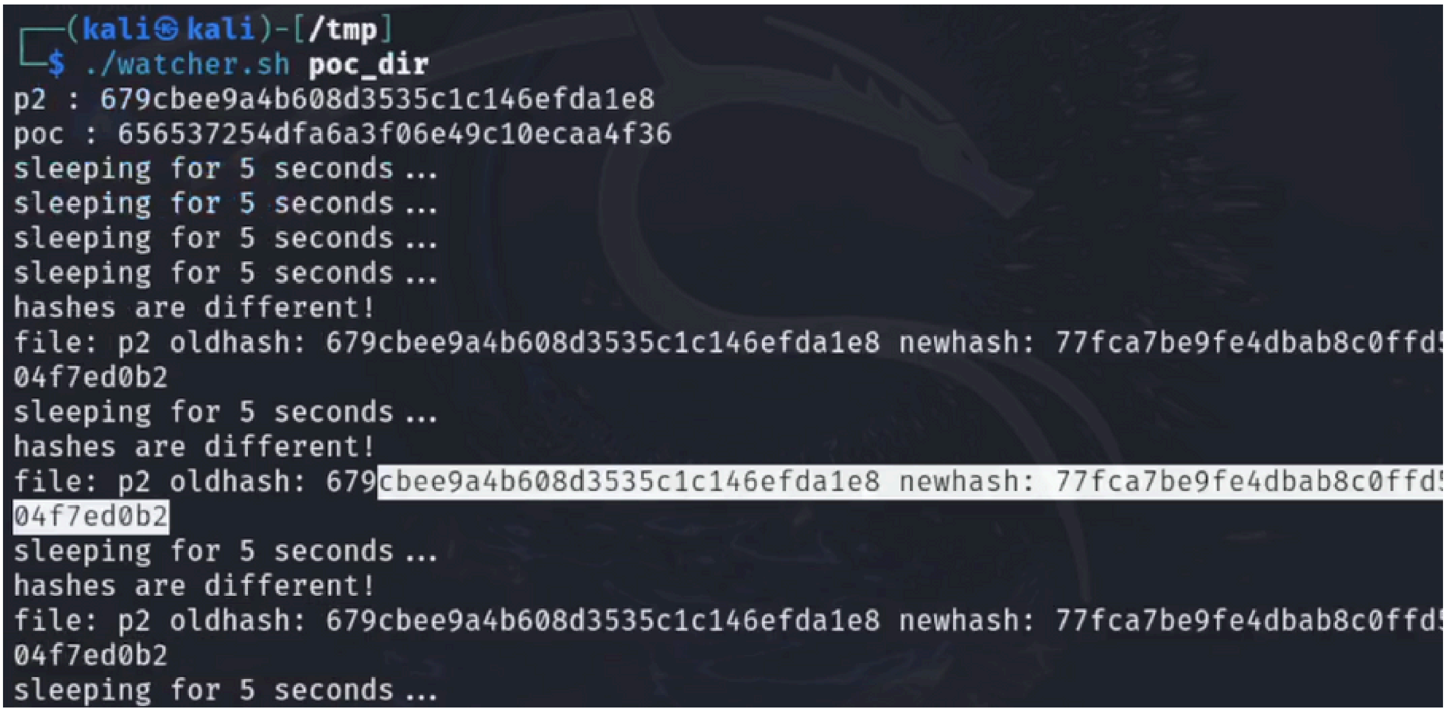
```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
p2 : 679cbee9a4b608d3535c1c146efda1e8
poc : 656537254dfa6a3f06e49c10ecaa4f36
sleeping for 5 seconds ...
sleeping for 5 seconds ...
```



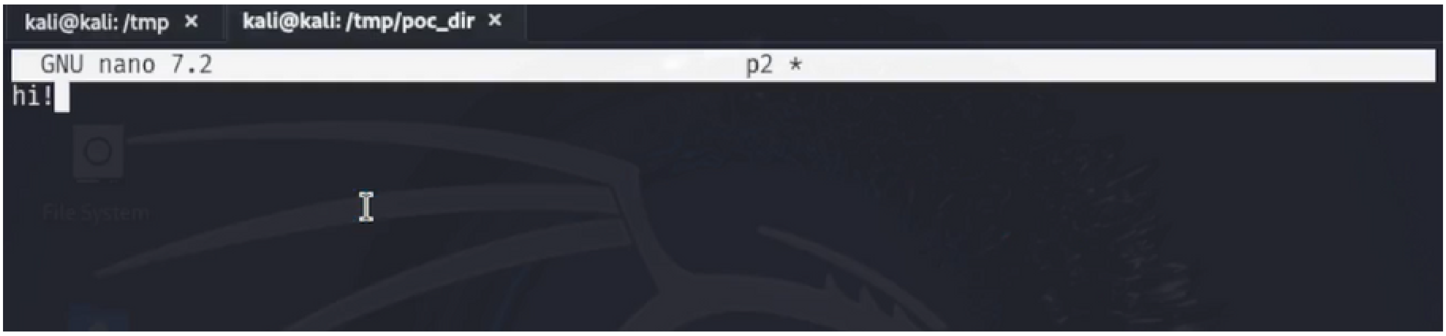
```
┌──(kali㉿kali)-[/tmp]
└─$ ls
poc_dir
ssh-j3CDHb9gwGCI
systemd-private-29ed3617135949b99c2c5b63fcfb1157-colord.service-BphxUO
systemd-private-29ed3617135949b99c2c5b63fcfb1157-haveged.service-p9Wqz2
systemd-private-29ed3617135949b99c2c5b63fcfb1157-ModemManager.service-GFRwre
systemd-private-29ed3617135949b99c2c5b63fcfb1157-polkit.service-rFfunC
systemd-private-29ed3617135949b99c2c5b63fcfb1157-systemd-logind.service-d0yfwq
systemd-private-29ed3617135949b99c2c5b63fcfb1157-upower.service-BCTf8x
watcher.sh

┌──(kali㉿kali)-[/tmp]
└─$ cd poc_dir

┌──(kali㉿kali)-[/tmp/poc_dir]
└─$ ls
p2  poc

┌──(kali㉿kali)-[/tmp/poc_dir]
└─$ nano p2
```



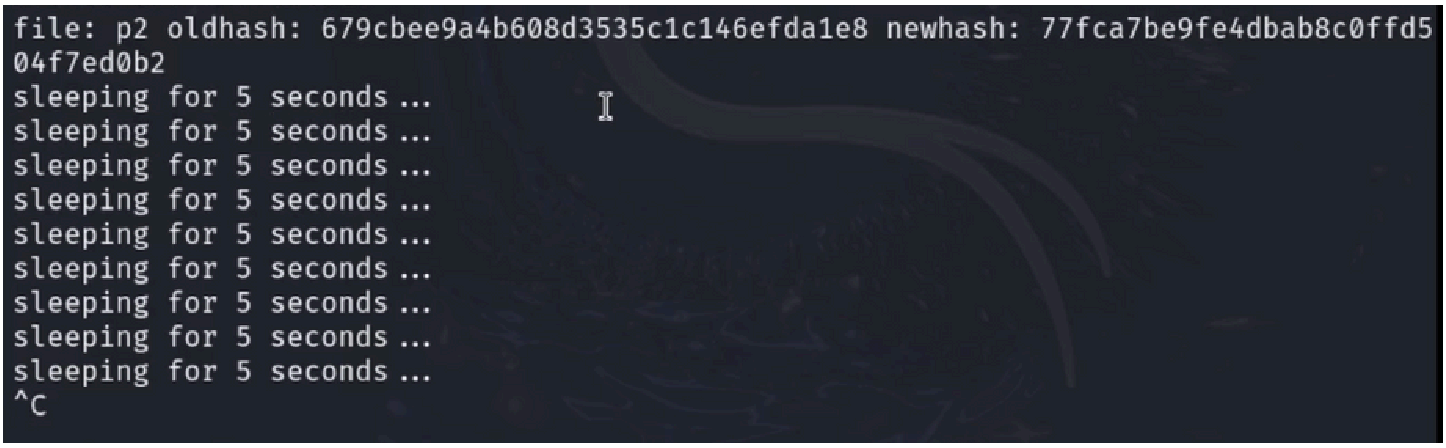
```
  GNU nano 7.2                                 p2 *
hi!2
```



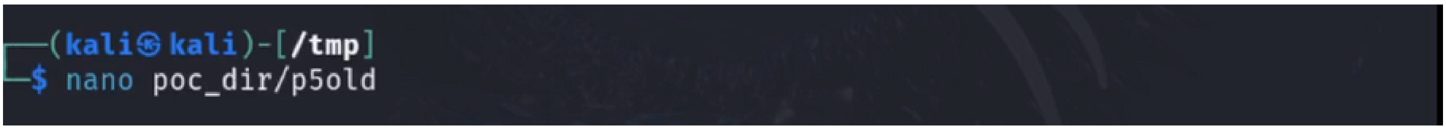
```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
p2 : 679cbee9a4b608d3535c1c146efda1e8
poc : 656537254dfa6a3f06e49c10ecaa4f36
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
hashes are different!
file: p2 oldhash: 679cbee9a4b608d3535c1c146efda1e8 newhash: 77fca7be9fe4dbab8c0ffd5
04f7ed0b2
sleeping for 5 seconds ...
hashes are different!
file: p2 oldhash: 679cbee9a4b608d3535c1c146efda1e8 newhash: 77fca7be9fe4dbab8c0ffd5
04f7ed0b2
sleeping for 5 seconds ...
hashes are different!
file: p2 oldhash: 679cbee9a4b608d3535c1c146efda1e8 newhash: 77fca7be9fe4dbab8c0ffd5
04f7ed0b2
sleeping for 5 seconds ...
```



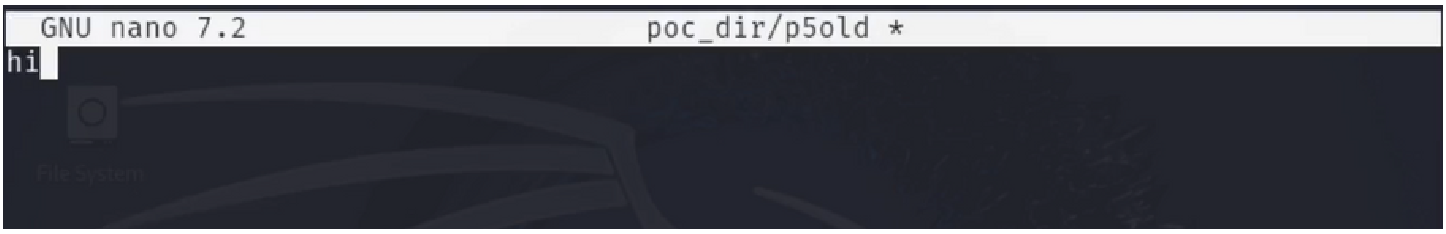
```
  GNU nano 7.2                                  p2 *
hi!
```



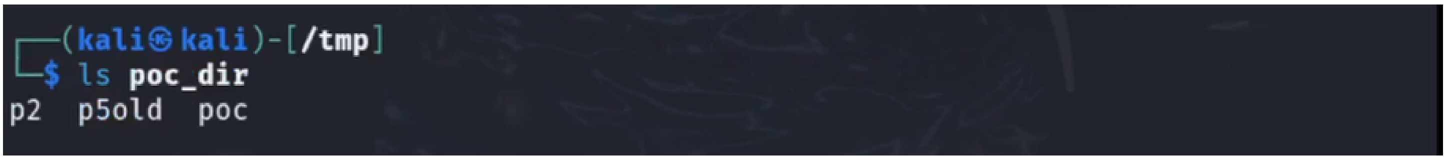
```
file: p2 oldhash: 679cbee9a4b608d3535c1c146efda1e8 newhash: 77fca7be9fe4dbab8c0ffd5
04f7ed0b2
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
sleeping for 5 seconds ...
^C
```



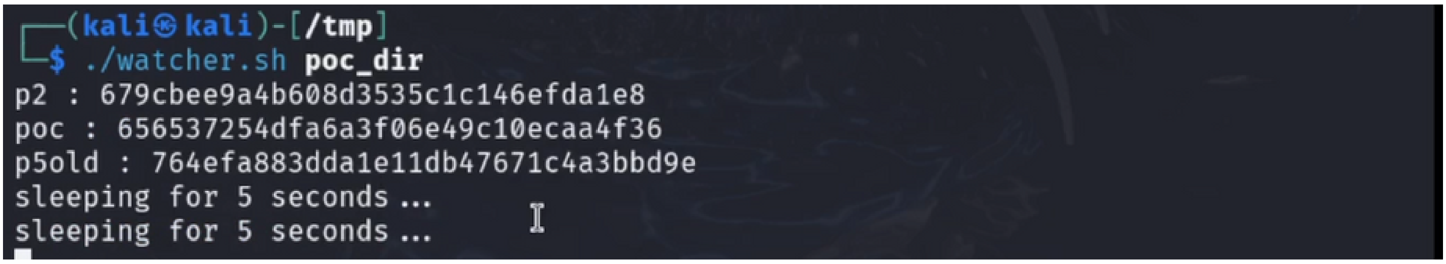
```
┌──(kali㉿kali)-[/tmp]
└─$ nano poc_dir/p5old
```



```
  GNU nano 7.2                         poc_dir/p5old *
hi
```



```
┌──(kali㉿kali)-[/tmp]
└─$ ls poc_dir
p2  p5old  poc
```



```
┌──(kali㉿kali)-[/tmp]
└─$ ./watcher.sh poc_dir
p2 : 679cbee9a4b608d3535c1c146efda1e8
poc : 656537254dfa6a3f06e49c10ecaa4f36
p5old : 764efa883dda1e11db47671c4a3bbd9e
sleeping for 5 seconds ...
sleeping for 5 seconds ...
```