Dirty COW (Dirty copy-on-write)

TCS 591 : Unit 2

What is a Dirty COW ?

- Dirty COW (Dirty copy-on-write)
- Dirty COW is a computer security vulnerability that affects all Linux-based systems, including "Android" devices(that used older versions of the Linux kernel created before 2018)
- It is a local **privilege escalation** bug that exploits a **race condition** in the implementation of the copy-on-write mechanism in the kernel's memory-management subsystem
- Dirty Cow was one of the first security issues transparently fixed in **Ubuntu** by the Canonical Live Patch service

What is a Dirty COW ?

- Dirty COW vulnerability is a type of privilege escalation exploit, which essentially means that it can be used to gain **root-user access** on any Linux-based system
- Dirty COW was a vulnerability in the Linux kernel. It allowed processes to **write to read-only files**. This exploit made use of a **race condition** that lived inside the kernel functions which handle the copy-on-write (COW) feature of memory mappings

What happen in a Dirty COW attack

- In Dirty COW Malicious programs can potentially set up a **race condition** to turn a read-only mapping of a file into a writable mapping.
- Thus, an underprivileged user could utilize this flaw to elevate their privileges on the system.
- By gaining root privileges, malicious programs obtain unrestricted access to the system.
- From there on, it can modify system files, deploy keyloggers, access personal data stored on your device, etc.

What Systems Are Affected By Dirty COW vulnerability ?

- Dirty COW vulnerability affects all versions of the Linux Kernel since version 2.6.22, which was released in 2007.
- According to Wikipedia, the vulnerability has been patched in kernel versions 4.8.3, 4.7.9, 4.4.26 and newer.
- A patch was released in 2016 initially, but it didn't address the issue fully, so a subsequent patch was released in November 2017.
- To check your current kernel version number, you can use the following command on your Linux-based system
  - $ uname - r
  - Major Linux distros like Ubuntu, Debian, ArchLinux have all released the appropriate fixes.

How Dirty COW Affects Android Devices

- ZNIU is the **first malware** for Android based on the Dirty COW vulnerability. It can be utilized to root any Android devices up to Android 7.0 Nougat.
- While the vulnerability itself affects all versions of Android, ZNIU specifically affects Android devices with the ARM/X86 64-bit architecture.