DIRTY COW

(CVE-2016-5195)
A Linux kernel Exploit

A Seminar Report

Submitted by

SUBHAJIT BARH
(18MA60R33)

in the partial fulfillment for the award of the degree
of

MASTER OF TECHNOLOGY
in
COMPUTER SCIENCE AND DATA PROCESSING
at

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR
WEST BENGAL-721302,INDIA

February 2019

ABSTRACT

Though Linux is lagging in the desktop user market(only 2.7 % user uses Linux according to a survey of November 2018) severs use Linux extensively. Around 80% servers use Linux as OS and popular mobile operating system like android also uses Linux kernel underneath it.

When in an operating system of that magnitude we found a security vulnerability it is really scary for all kind of reasons. Though Linux is in over all really a secure operating system than its counterparts but it also had its bad days.

2016 November was a nightmare for Linux developers because in that month Dirty COW(CVE-2016-5195) was discovered by a security researcher named Phil Oester. It was an Privilege Escalation Vulnerability and it utilized race condition to exploit an ancient flaw in the linux kernel. Linux Kernel version 2.6.22 (Released in 2007) to kernel 4.8.3 (in 2017) are vulnerable. Now Linus Torvalds the father of the Linux project said that he discovered it(the BUG) a long time ego and tried to fix it in vain he termed it as theoretical vulnerability. But it is not theoretical any more .

Linux Developers tried to fix the BUG in 2016 hurriedly but was not a complete success The patch was not full proof. In 2017 it was fully patched and it is Dirty COW free from Linux kernel 4.15(UBUNTU 18.04).

So staying updated is the only defense we have in this scenario. Thus in this seminar report I will try to explain what was the bug , how it was exploited and what we can do about it .