

Lab 6: Proof of Concept (POC)

Operating Systems Exploitation

Table of Contents

[Lab Outcome 2](#_Toc530412564)

[The Exercise 2](#_Toc530412565)

[Submission – Lab 6: POC 3](#_Toc530412566)

Operating Systems Exploitation

Lab 6: Proof of Concept (POC)

# Lab Outcome

Review existing POCs related to security vulnerabilities, exploits and its documentation.

# The Exercise

Find and research about a specific security POC:

1. What is the security vulnerability?

**CVE-2016-2384: Exploiting a double-free in the USB-MIDI Linux kernel driver**

1. What kind of device or software is the vulnerability affecting?

**USB-MIDI Linux kernel module**

1. Review the POC and all the documentation (program, manuals, license, etc…). Briefly describe each one of them

**The bug**

**“**The issue with the USB-MIDI driver is a double-free of a snd\_usb\_midi object, which occurs when a Midiman USB device with invalid number of endpoints is plugged in.”

**Exploit**

* Denial of service
* Arbitrary code execution

**Kernel hardening**

* Supervisor Mode Execution Protection & Supervisor Mode Access Prevention
* Kernel Address-Space Layout Randomization

**SMEP bypass**

* Exploit that uses Return oriented programing.

1. Analyze each section of the POC like the published vulnerability, requirements, how to use, scope, vulnerable versions, mitigation techniques, licenses and copyright

**Published vulnerability**

* CVE-2016-2384
* <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2384>

**Requirements**

* The CPU supports it
* The kernel supports it
* It’s enabled in the kernel configuration

**How to use**

* Exploit to privilege escalation or even a device to do Denial of service.

**Scope**

Prevention/hardening

**Vulnerable versions**

* Ubuntu 14.04 (3.19.0-49-generic),
* Linux Mint 17.3 (3.19.0-32-generic),
* Fedora 22 (4.1.5-200.fe22.x86\_64)
* CentOS 6 (2.6.32-584.12.2.e16.x86\_64).

**Mitigation techniques**

* Updating
* Kernel hardening

**Licensing/** **Copyright**

* GNU General Public License version 2 only (GPL-2.0)

1. Find one or more sections of the POC that can be improved, explain the reasons to improve the POC and provide any changes that you will implement to the POC as a new version

In my opinion, the POC could be improved is a demonstration of the kernel hardening. Showing the public that will show average person how to do it.

1. Submit your work

**Due date: Dec 3, 18**

# Submission – Lab 6: POC

Submit it to D2L

Weight: 6 %