

Lab 5: Bootkits

Operating Systems Exploitation

Table of Contents

[Lab Outcome 2](#_Toc494699707)

[Introduction 2](#_Toc494699708)

[1.0 Kitgen 2](#_Toc494699709)

[2.0 Reference 2](#_Toc494699710)

[3.0 Sign-Off – Lab 5: Bootkits 3](#_Toc494699711)

Operating Systems Exploitation

Lab 5: Bootkits

# Lab Outcome

Examine bootkit techniques.

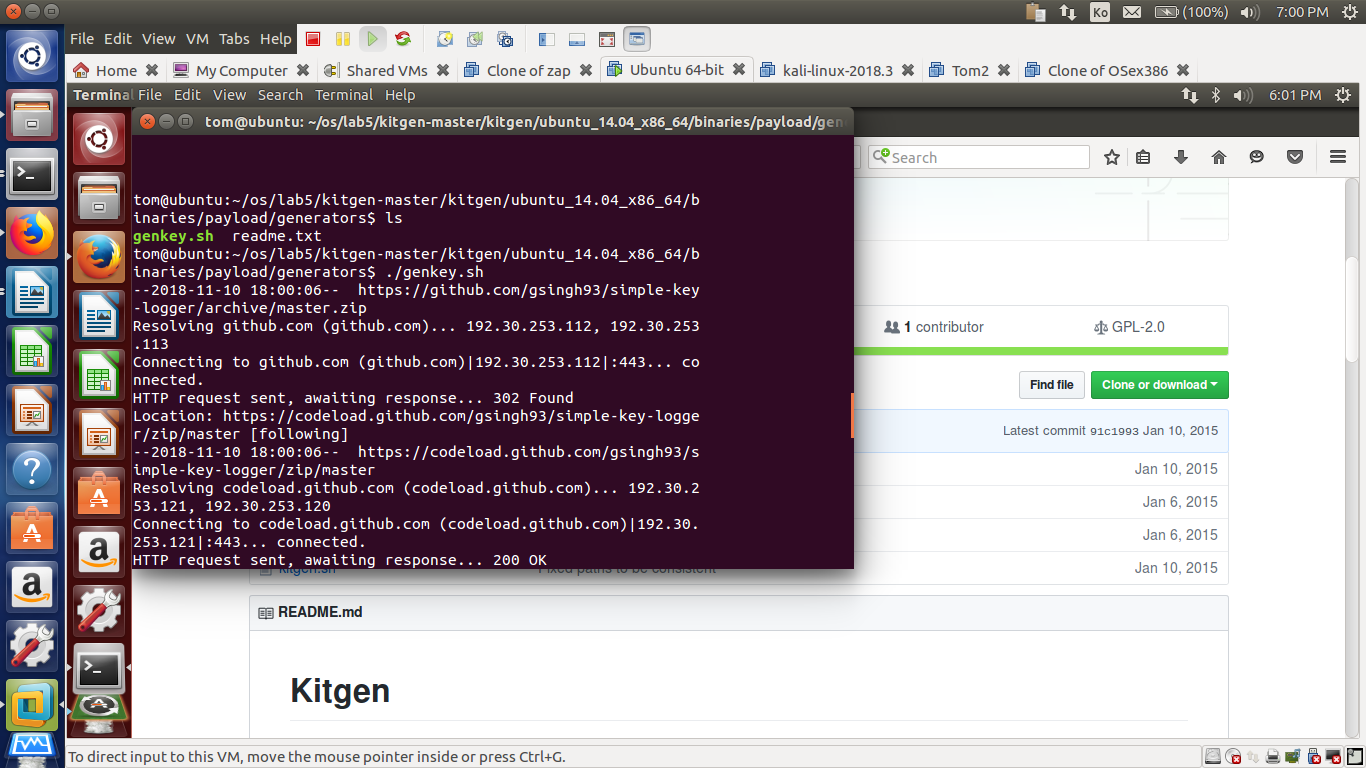
# Introduction

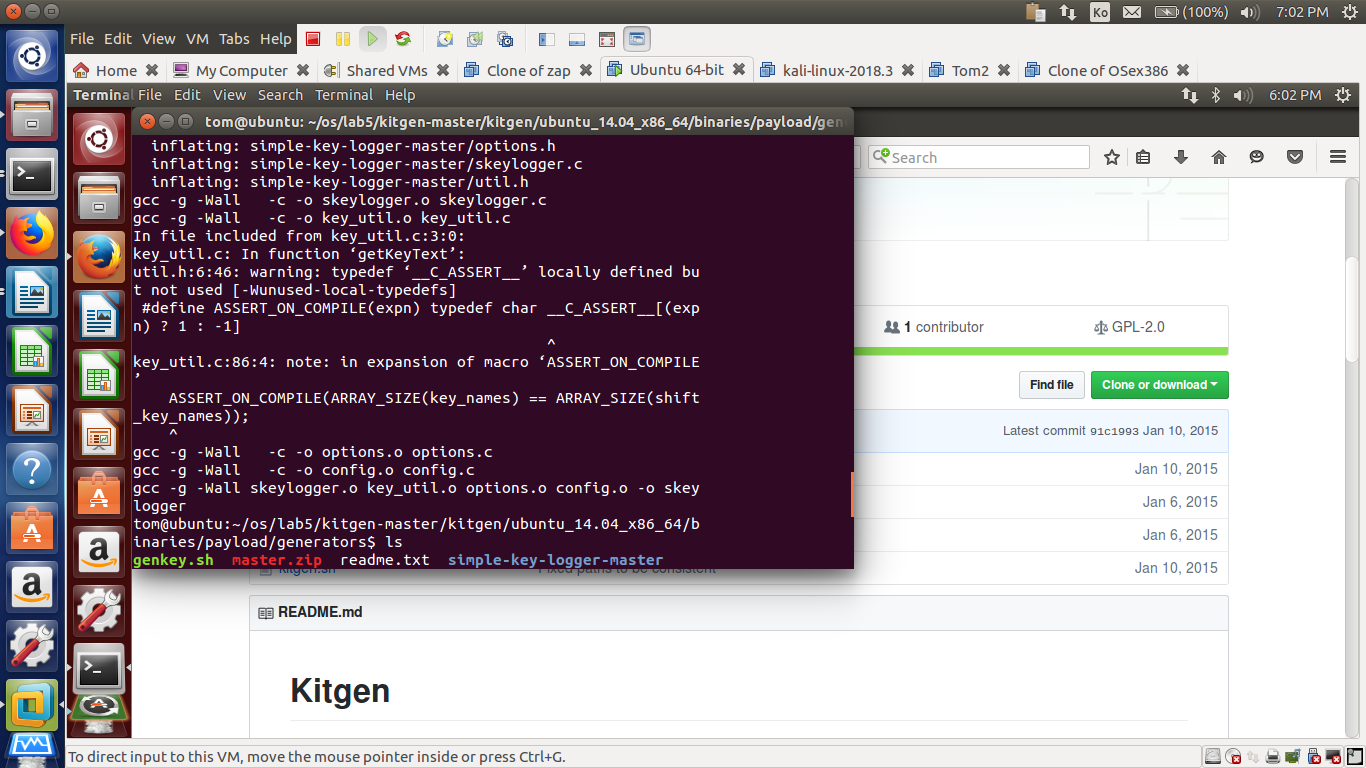
Firmware rootkits leverage a device’s firmware to inject malicious code into the hardware. Often, firmware rootkits go undetected because the firmware is rarely inspected for integrity. “A bootkit is a malicious program that infects the early stages of the system startup process before the operating system is fully loaded” (Matrosov, Rodionov, & Bratus, 2017). Bootkits are difficult to detect because they are beyond kernel control. They are almost impossible to remove because doing so can damage the entire system.

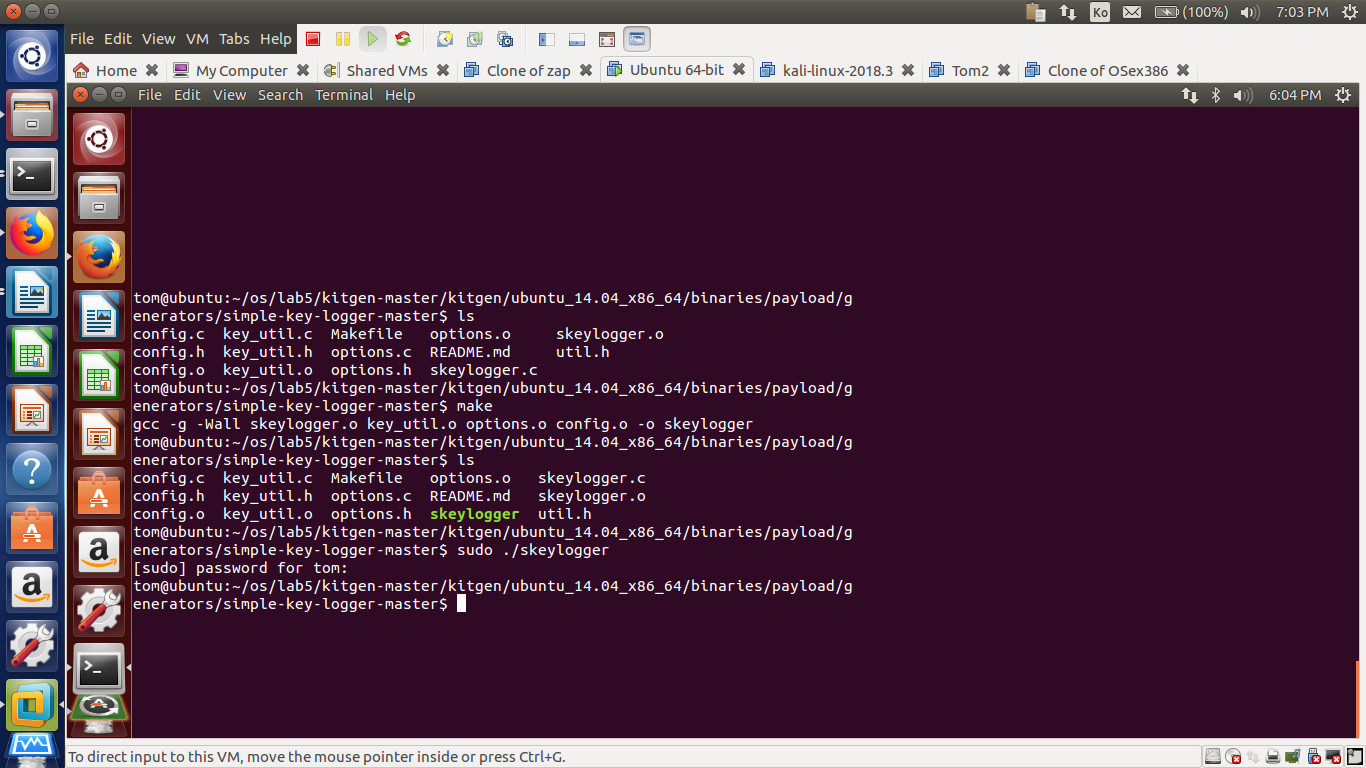
# 1.0 Kitgen

There are many sample bootkits available online. Some have been used to infect actual systems. Others are examples created for educational purposes. This lab deals with the latter.

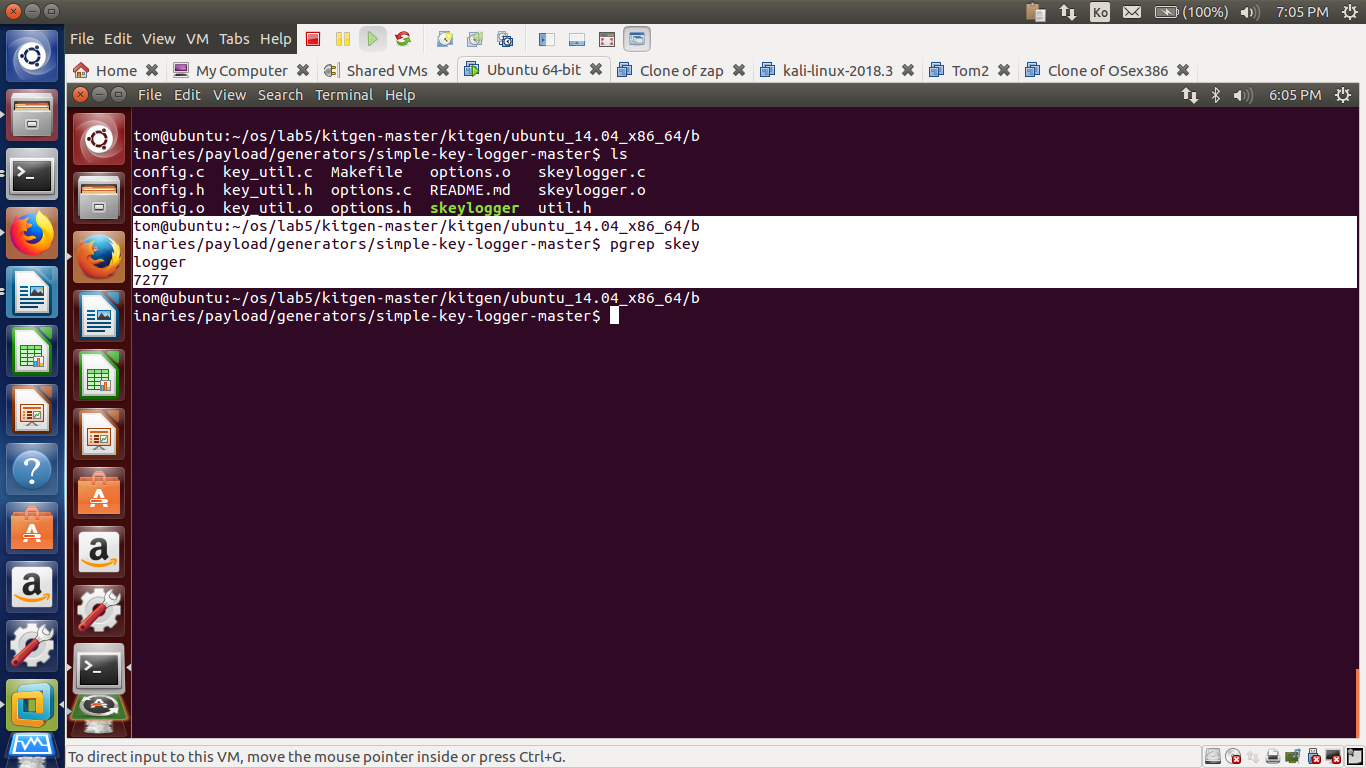
1. Go to [Linux bootkit generator](https://github.com/chesteroni/kitgen) (https://github.com/chesteroni/kitgen) and download the source code of this Linux bootkit.
2. Follow the instructions to generate a bootkit to infect the initrd files on your Ubuntu system.

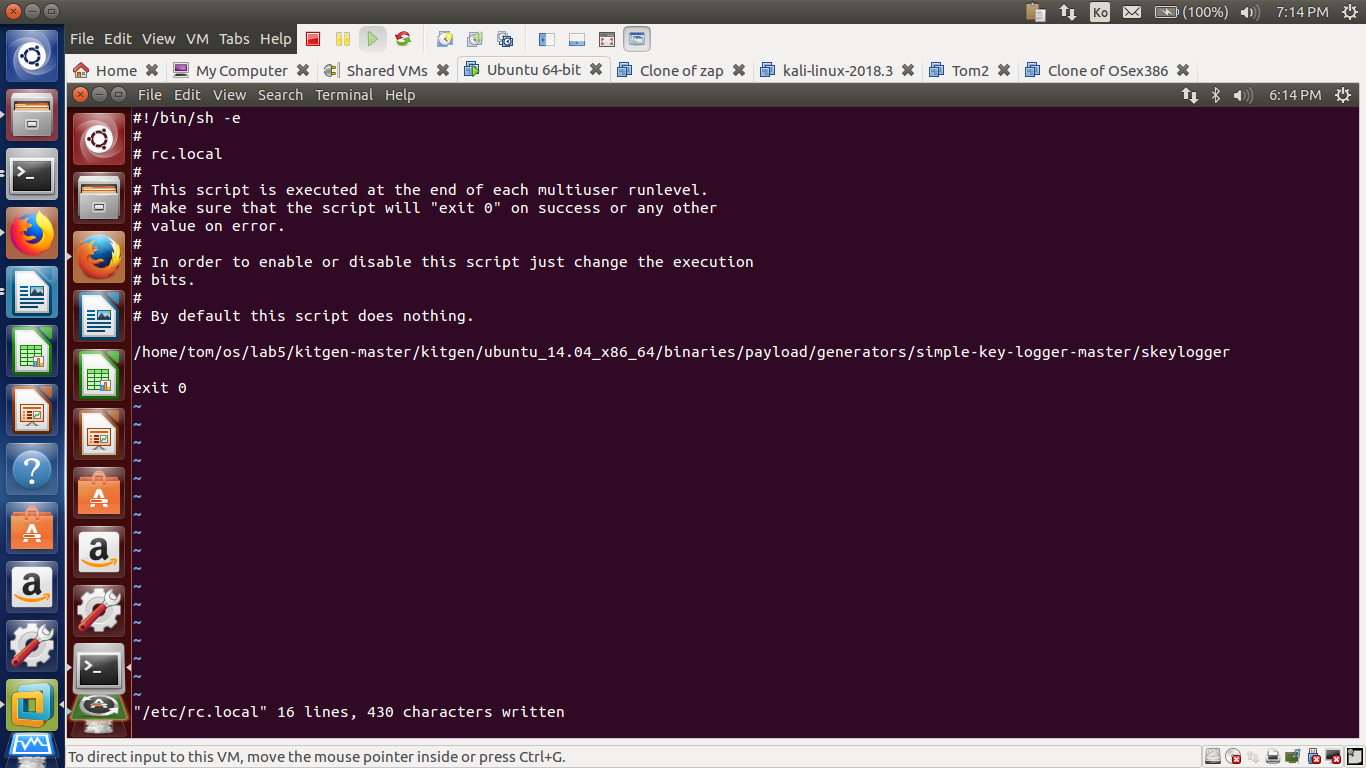


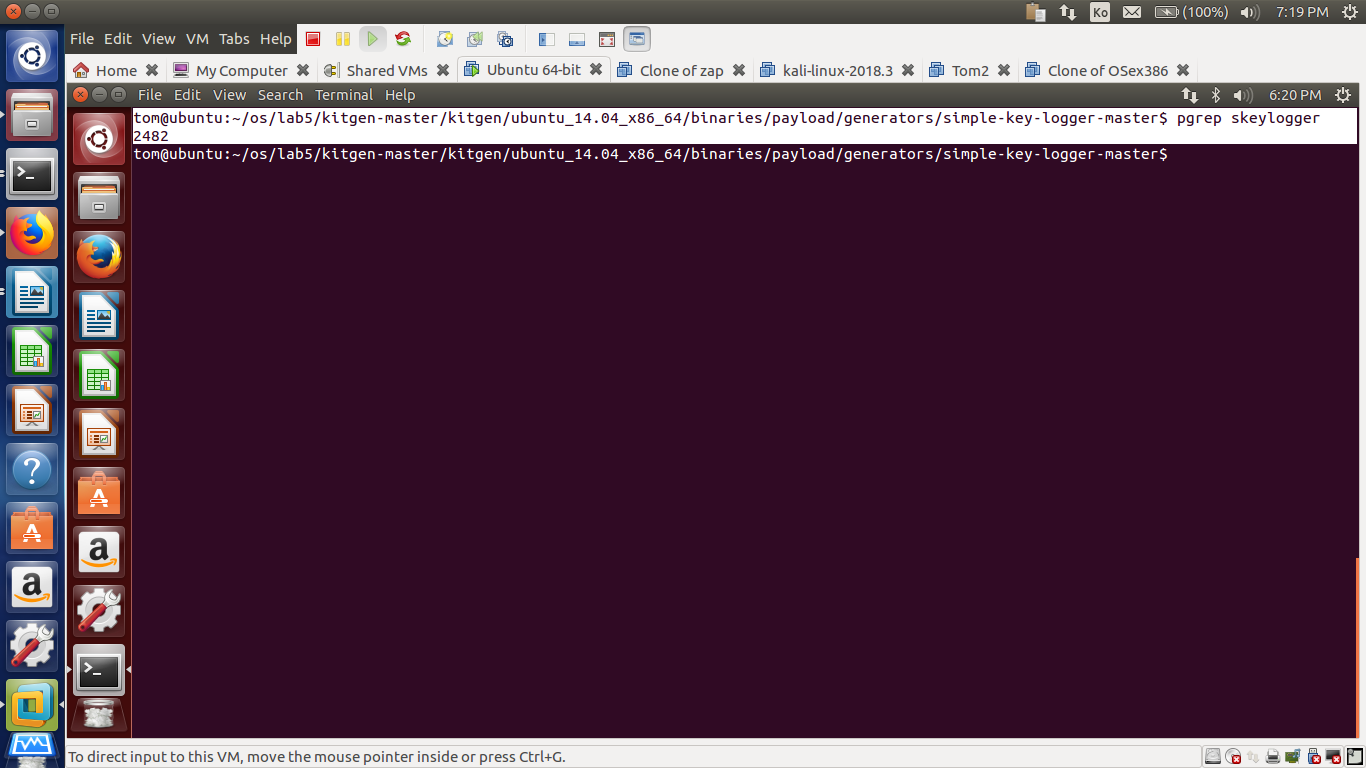
****

****

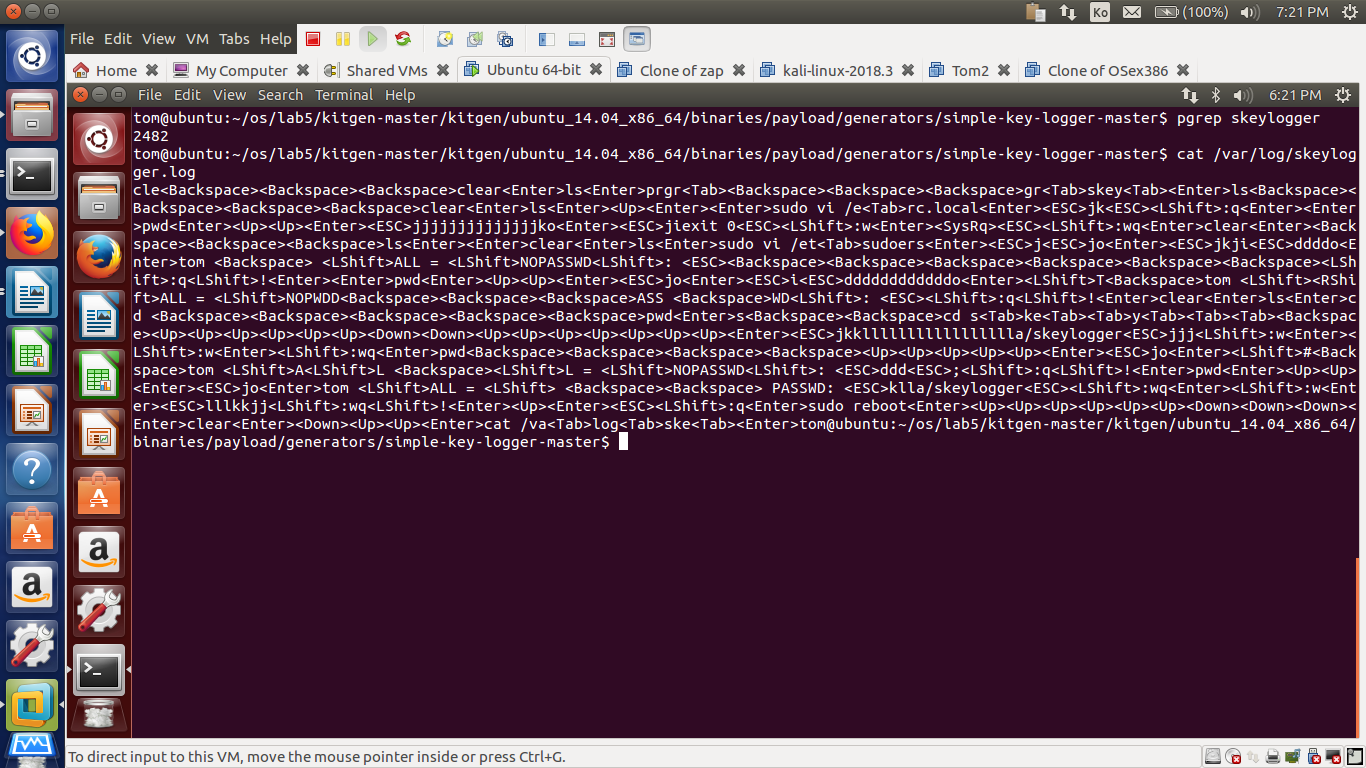
**executable “skeylogger”**



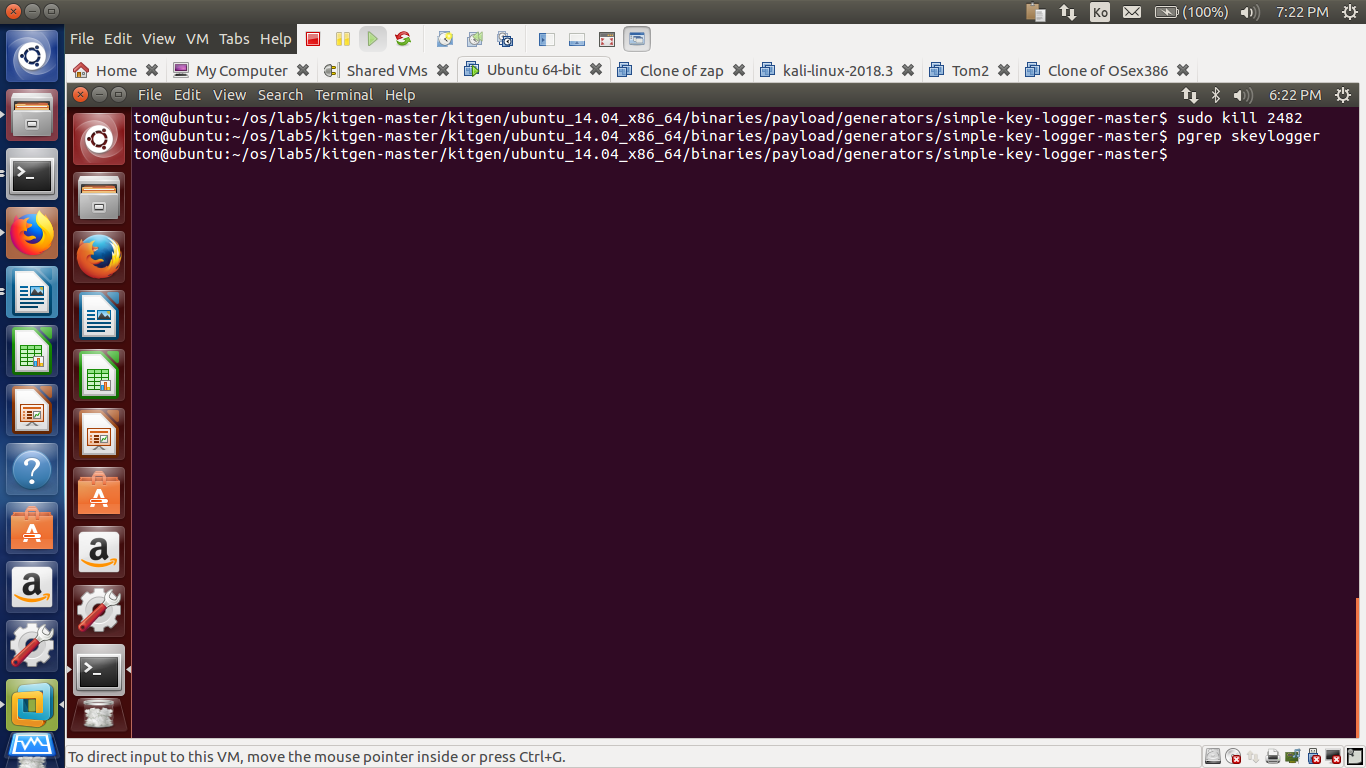




**After rebooting the skeylogger was still running**



**I opened up the skeylogger.log file to check if the keylogger actually plays its role.**



# 3.0 Submission – Lab 5: Bootkits

Submit it to D2L

Weight: 6 %