**Fredrick Onduso Ondieki**

**CST-221 Operating System Concepts**

**CST-221 Security**

**John Zupan**

**April 16, 2019**

**Git hub Link:** **https://github.com/FREDDYSMALLZ/Operating-Systems-Concepts-CST-221.git**

**CST – 221 Security**

Activity Directions:

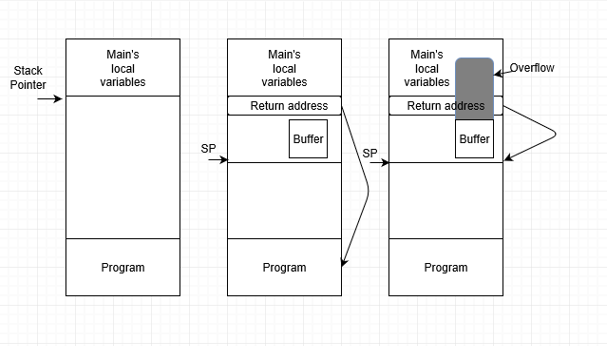
In this project assignment we were required to do research on Linux Security as well as develop some bash scripts to support Linux System Administration. The following are the tasks that were done to complete the assignment successfully:

* Buffer Overflow, Diagram, Issues and Harm that Buffer overflow causes, and techniques used to prevent buffer overflow.
* Zero Day exploit; Article reading, Modernism, Christianity and Business Ethics
* Kali Linux, how it is used to train security professionals, Table that lists the standard tools included in the Kali distribution and world view perspective.
* Script bash to test for password strength.
* Bash Script to manage users.

**Buffer Overflow**:

Buffer overflow is the situation/condition in which a program attempts to write data beyond the boundaries of pre-allocated fixed length buffers. The excess written data is put to the adjacent memory overwriting the available content which in return causes the program to behave in unusual manner thus producing unpredictable results. Buffer overflow condition occurs when no validation bounds are put in place prior to data being written (Buffer Overflow, 2019).

**Buffer Overflow diagram**



(Tenenbaum & Bos, 2015)

**Issues and harm that a Buffer Overflow can cause and how this is feasibly possible in a C program.**

Buffer overflow crashes programs or in its “lenient” phase, the program will slow down instead of crashing. For some reason, (Not common today), the program will return bad data which commonly experienced when running games which are poorly designed. For example, the when run the ***Tomb raider*** (Released in 2016)game on 4 gigabytes memory, it will crash and for some reason it can run on 3 gigabytes memory. This is a sign of poor development. The worst case is that buffer overflow can inject commands to the overflow causing other programs to run and commands executed. Therefore, hackers can use the overflowed data and write code outside the buffer and then in return overwritten to the stack as well as commands thus giving the hacker room to exploit the system.

Buffer overflow can easily occur in C programs since C is a lower-level programming language. C allows direct memory access by various programs. This is not beneficial as data can be overwritten by the programs. “…Note that there is some amount of circular reasoning involved: Security issues are frequently linked to C and C++. But how much of that is due to inherent weaknesses of these languages” (DevSolar, 2016). Lastly, C language brings about the issue of machine language. During compilation, the C programs are directly compiled into the native machine language of the CPU. The effect is that the erroneous code can overwrite program memory or stack and thus execute instructions not in the original program.

**Techniques that are used to prevent, defeat and defensive mechanisms to overcome Buffer Overflows**

One technique that is used to ensures that a Buffer Overflow does not occur, is to authenticate the values that the user enters to the program. When developing applications developers and programmers must make sure that values entered by a user are properly validated by ensuring that the right length string does not exceed or go beyond the pre-set length of characters. Going beyond those characters would result to thwarting the unauthorized user by segmentation fault even if the user uses the buffer overflow technique. Segmentation fault is a process that occurs when a process tries to access memory that is not mapped to its address space (Love, 2013).

**Zero Day Exploit**

A zero-day exploit is a security flaw or hardware/software vulnerability which is exploited by hackers or attackers releasing malware not giving developers the opportunity to create a patch to fix the vulnerability (What is a Zero-Day Exploit? Zero-day exploit: An advanced cyber-attack defined, 2019). The term "zero-day" means that developers/programmers have had zero days to fix the vulnerability. In addition, According to Perlamo, 2013, zero-day exploit occurs because the developer is not aware that there is an issue that is present on the application until problem manifests itself. Bellow are the steps for vulnerability window:

* An organization or company developer create programs/software, but unbeknownst to them it contains a vulnerability.
* The threat actor spots that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
* The attacker writes and implements exploit code while the vulnerability is still open and available.
* After releasing the exploit, either the public recognizes it in the form of identity or information theft or the developer catches it and creates a patch to staunch the cyber-bleeding (What is a Zero-Day Exploit? Zero-day exploit: An advanced cyber-attack defined, 2019).

**Latest Zero-Day Exploits**

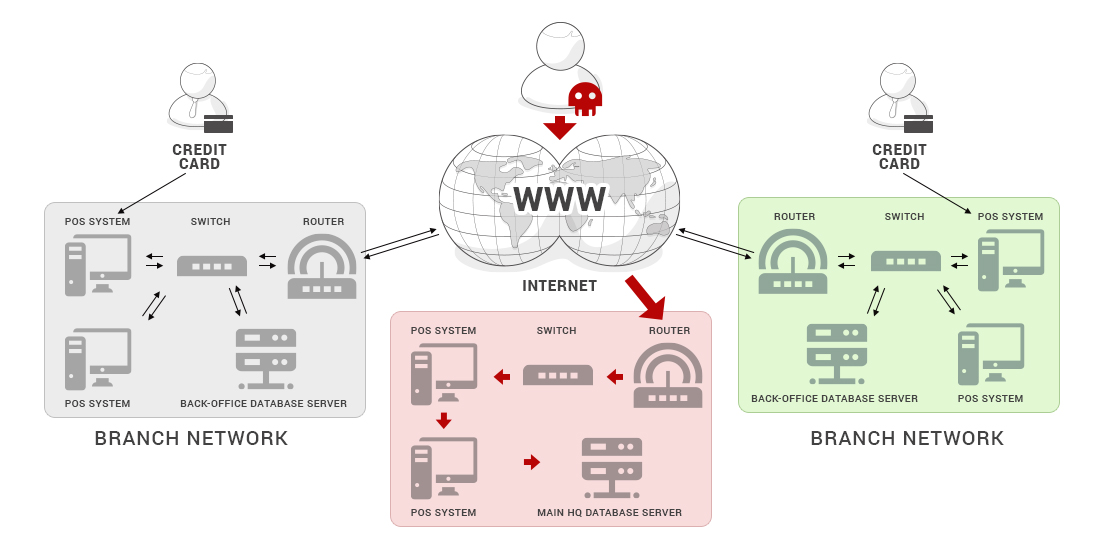
**Windows**: There was a zero day that was identified by a Google security engineer in the latest support releases of Windows OS. He says the code was not right for the past 20 years.

**Java**: Oracle came up with emergency patch releases to fix critical vulnerability issues on Java based platform in March. The vulnerability has been the preying target for hackers. Both Windows and Mac devices are considered prone to this risk.

**Acrobat Reader**: The security experts were surprised to discover a zero-day exploit that was created to sneak into sandboxed environment of the Adobe reader 10 and 11 in February. The security experts are convinced that the vulnerable exploit is mostly considered to be virtual spying tool created by government agencies and are highly sophisticated.

**How to prevent zero-day exploits**

* Update all the applications and software once the security patches are released
* Implement the use of Web Application Firewall (WAF) to protect your website. It helps to identify possible website attacks with much accuracy
* Install Internet Security suite that is loaded with smart antivirus, sandboxing techniques, default deny protection, heuristic file behavioral analysis.



The vendors are also notified on the latest patch and they are to rectify the software bug by updating the software with the security patch fix. There is alternative option, where the vendors can automate the software updates as and when an update is released. Zero-day exploits can also be avoided by choosing an antivirus solution that defies both known and unknown threats (What is Zero-Day Exploit (Attacks)? 2019).

**How ethical issues can arise in a Zero-Day Exploit and how this knowledge could be used to benefit you or others around you.**

When zero-day exploit occurs, you are the first person to know of it. This means that you have the very power to decide whether to get money from it or be the ethical thing to report it so that the issue that the software has cannot harm those around you. By doing so, the developers can have time to fix the problem. Sharing the zero-day exploit to a third party and end up being caught with stolen material, both of you will be treated as thieves and an accomplice to the crime. From the Cristian point of view, it is unethical for people to seek monetary gain by exploiting work that has been done by another person.

Also, it is an act of stealing. One of the ten commandments forbid against stealing. Learning or having the information about zero-exploit can make a person rich, but the party included need to remember that it is not your work or sweat as it is stolen information.

Lastly, zero-day exploit goes against the concept of work which was ordained by God. By exploiting the sweat of others, it is an act of sinning and not being honest to your creator and self. The exploit itself is a disgrace to the very definition of work and not reporting it is unethical.

**Kali Linux**

**Kali Linux is and how is this used to train security professionals.**

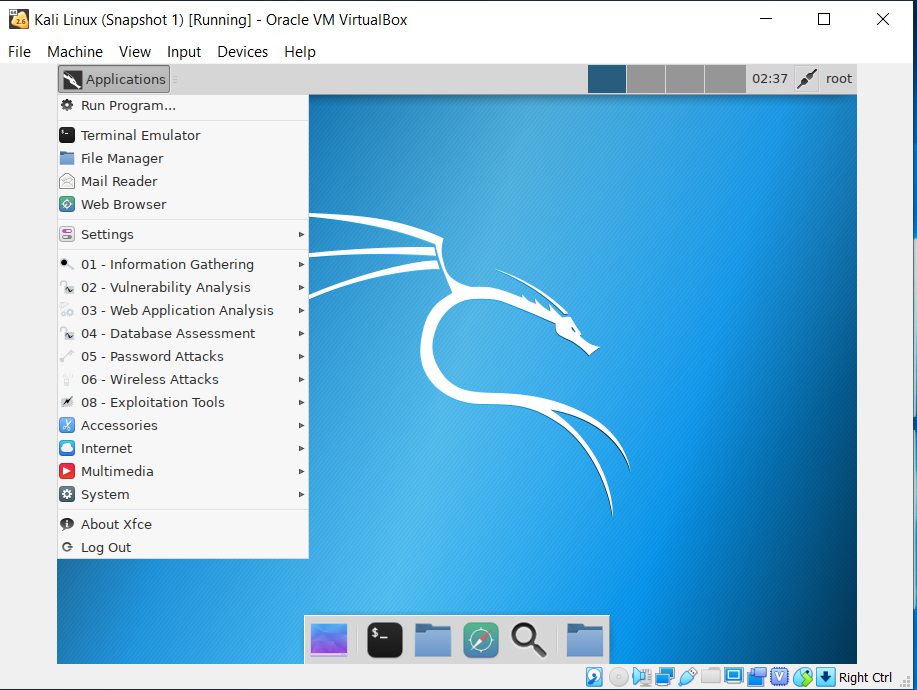
Kali Linux is a distribution system geared towards providing advanced Penetration Testing and Security Auditing. It is also a distribution system geared towards ethical hacking and penetration. Kali Linux contains hundreds of tools aimed at assisting security professional in penetrating systems. Kali system was built to train security professionals on Linux based system on how they can penetrate system, provide security features and realize the ways in which hackers can exploit the system.

Kali Linux is made by Offensive Security. They provide a training courses that are highly sought-after certification, OCSP. The training is knowledge based aimed at how the student understands the concepts taught. Most of the time, the students (Security professionals) spend time in attempting to penetrate computer systems. The objective here is to make sure that the induvial master the security concepts and how the tools work (Penetration Testing Training with Kali Linux, 2018).

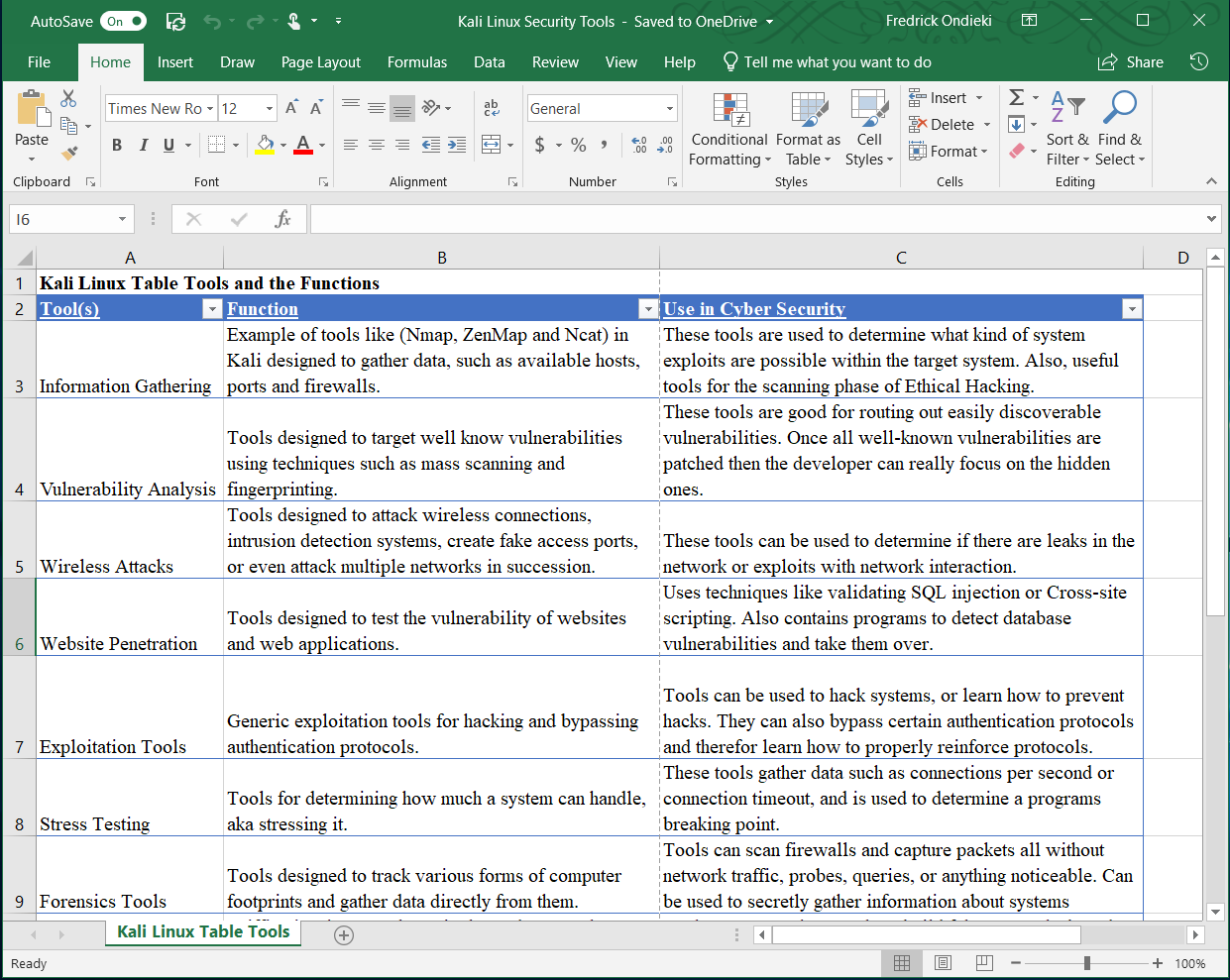
**Table that lists the standards tools that are included in the Kali distribution and how the tool is used in cyber security training.**

There are numerous Kali Linux tools out there which have different functions. These tools are categorized according the function they do and how the security professional use. These categories are:

* Information gathering tools-Amap, APT2, Automater
* Vulnerability analysis tools-Cisco-ocs, BED, BBQ, BBQSQL
* Web application analysis tools--Apache-users, Arachni, BBQSQL,Grabber
* Database assessment tools-sqlmap,
* Password attack tools-
* Wireless attacks tools--Airbase-ng, Aircrack-ng, Airplay-ng
* Exploitation tools-Commix, Cisco-ocs, Armitage



The screen shot bellow shows the table of the Kali Linux tools. The data on the table is includes as a spreadsheet attachment.



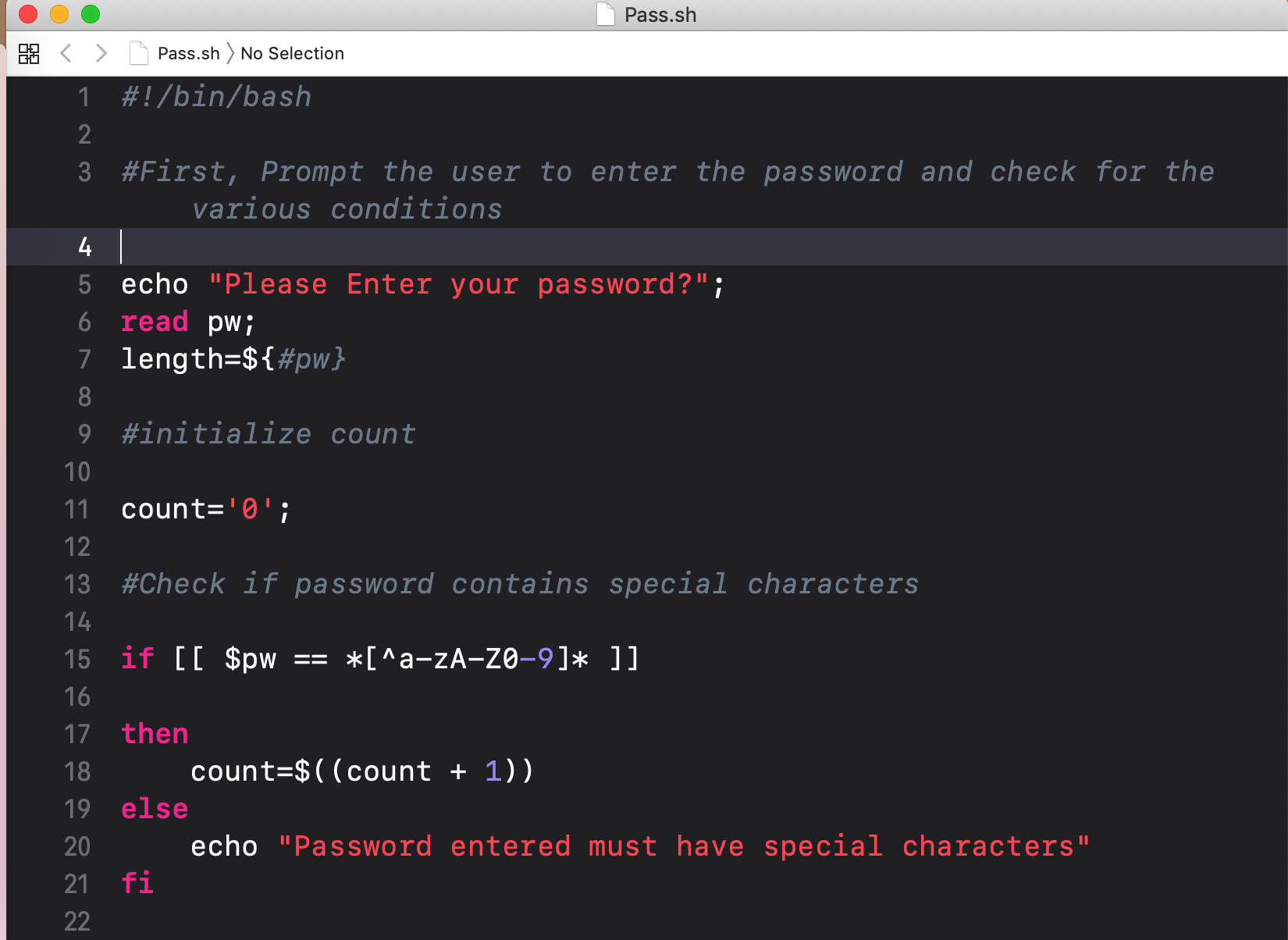
**Ethical issues that could arise related to knowing and using a system like Kali Linux and how this knowledge could be used to benefit you or others around you.**

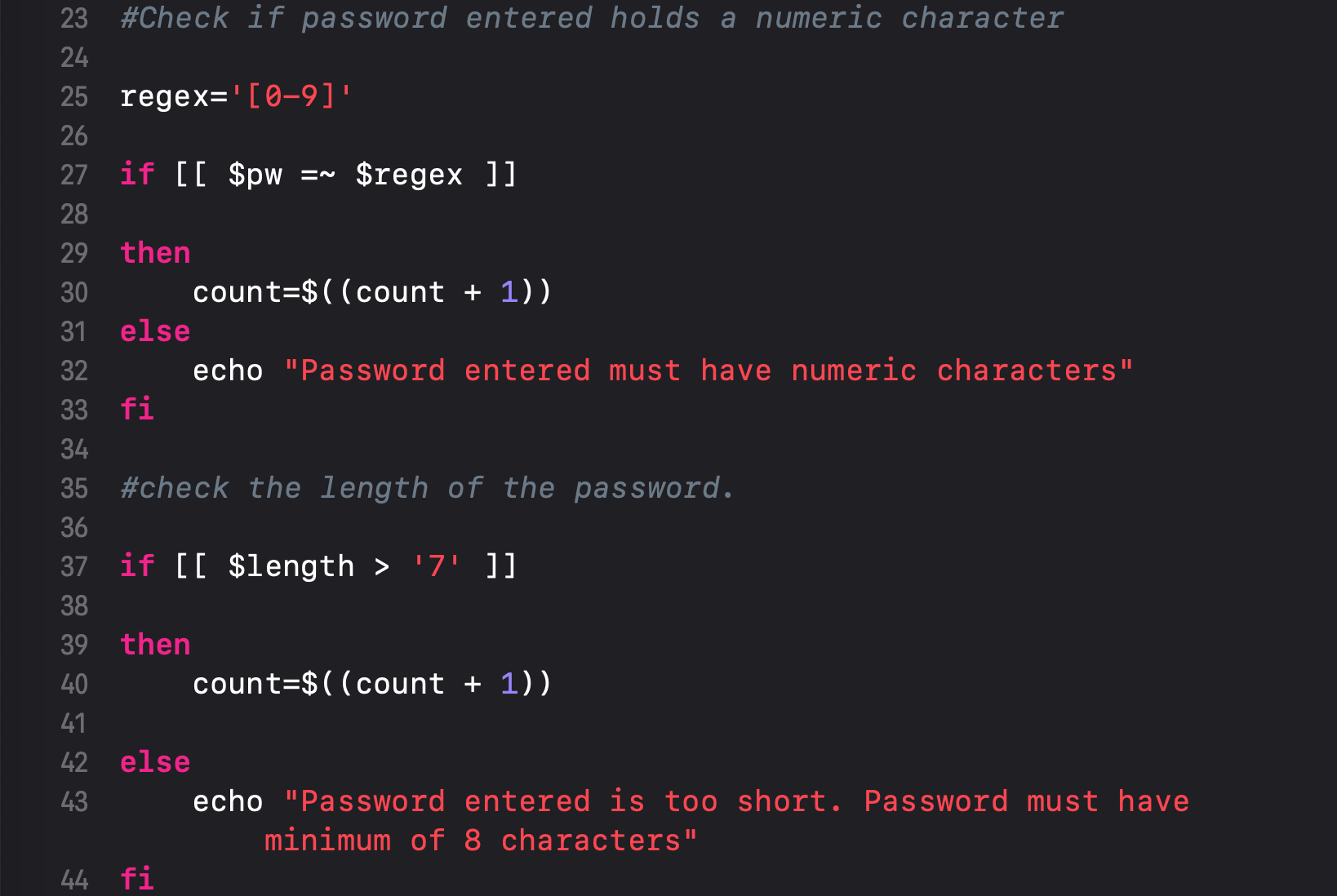
Kali Linux tools has numerous tools that can be used both for ethical and other wrong purposes if the knowledge gained can be exploited by hackers. This is due to the different number of tools as we have seen above which perform different functions with the aim of penetrating the computer system. Ethically, the knowledge gained can be used for research purposes meaning that it can used to prevent hackers from penetrating systems. Above all, this knowledge can be used to develop programs that are secure, and users can use without having the fear that their data can be compromised.

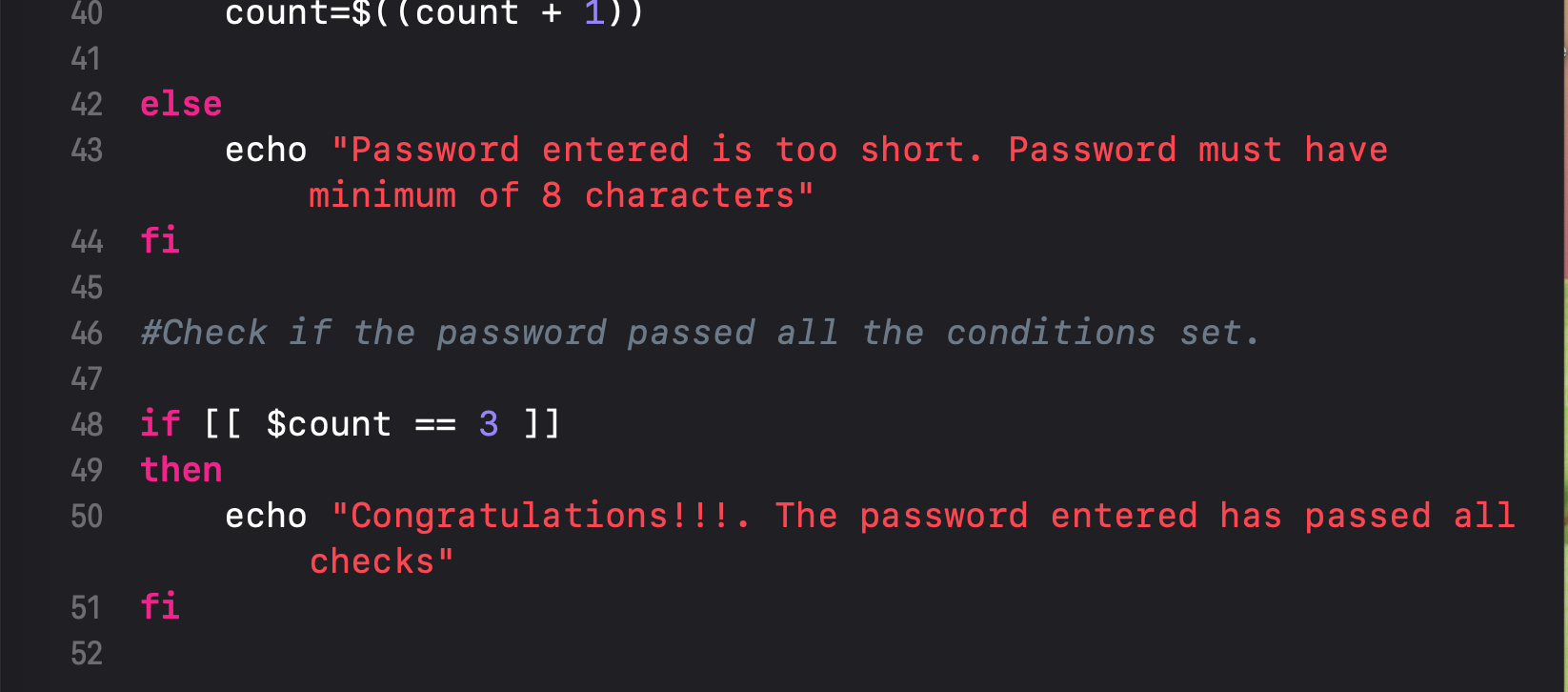
However, if someone is gaining Kali Linux knowledge to penetrate and access systems that has already been established, then the person is acting unethically. Even though there may be monetary gain from cracking passwords, getting other people data and selling them, then this is unethical as it is stealing in nature and one may be prosecuted.

Lastly, from the Christian point of view, stealing something such as data and information goes against the Christianity laws and breaks the commandments of God which bars people from stealing. Penetrating people’s networks, computer systems without the consent of the person is wrong and is something that Christians should not do. Since the tools offer different functions, the absolute choice on how to use the knowledge of this tools falls on the user. Thus, choose wisely and consider other people’s feelings.

**Script to test for password strength:**

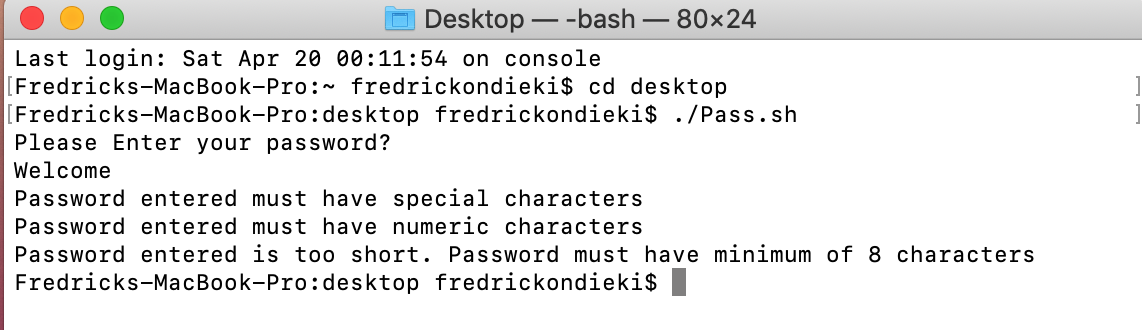
The screenshots bellow shows the code used for the bash script for testing password strength and its execution. 

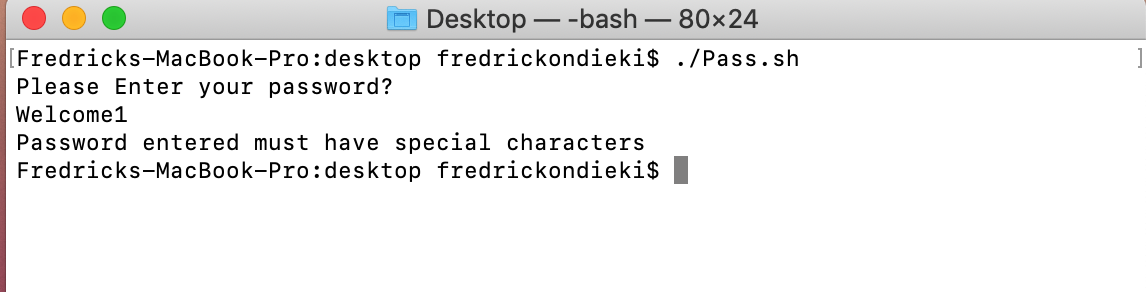


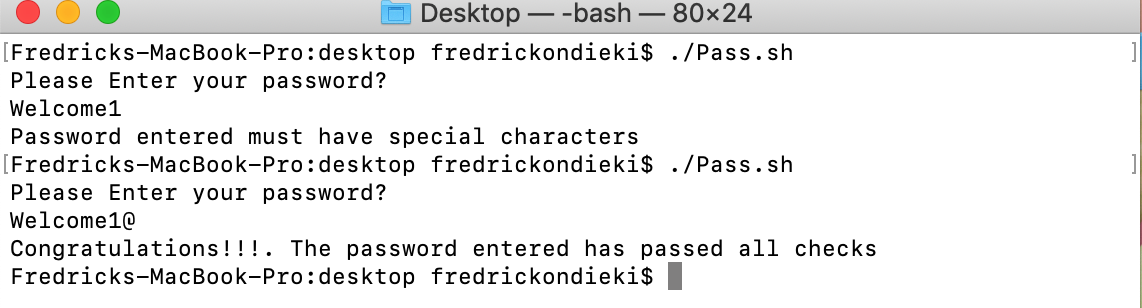


**Script bash code execution**

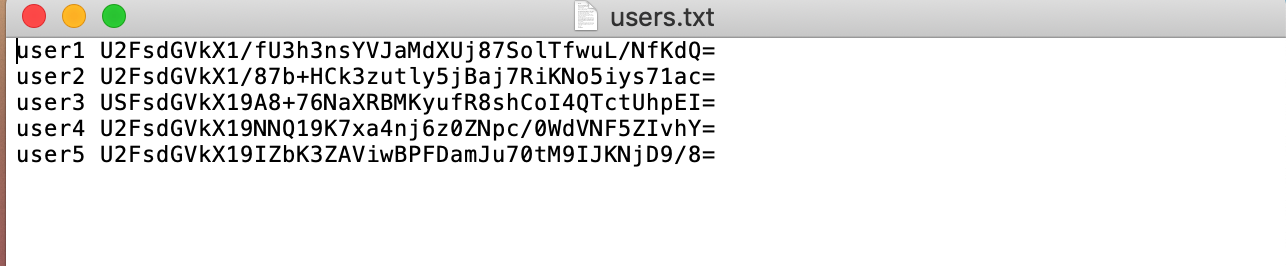
The above code performs checks such as if the user’s password has 8 characters, at least one numeric and non-alphanumeric characters and flags “weak’ or easily suggested passwords guessed by individuals.

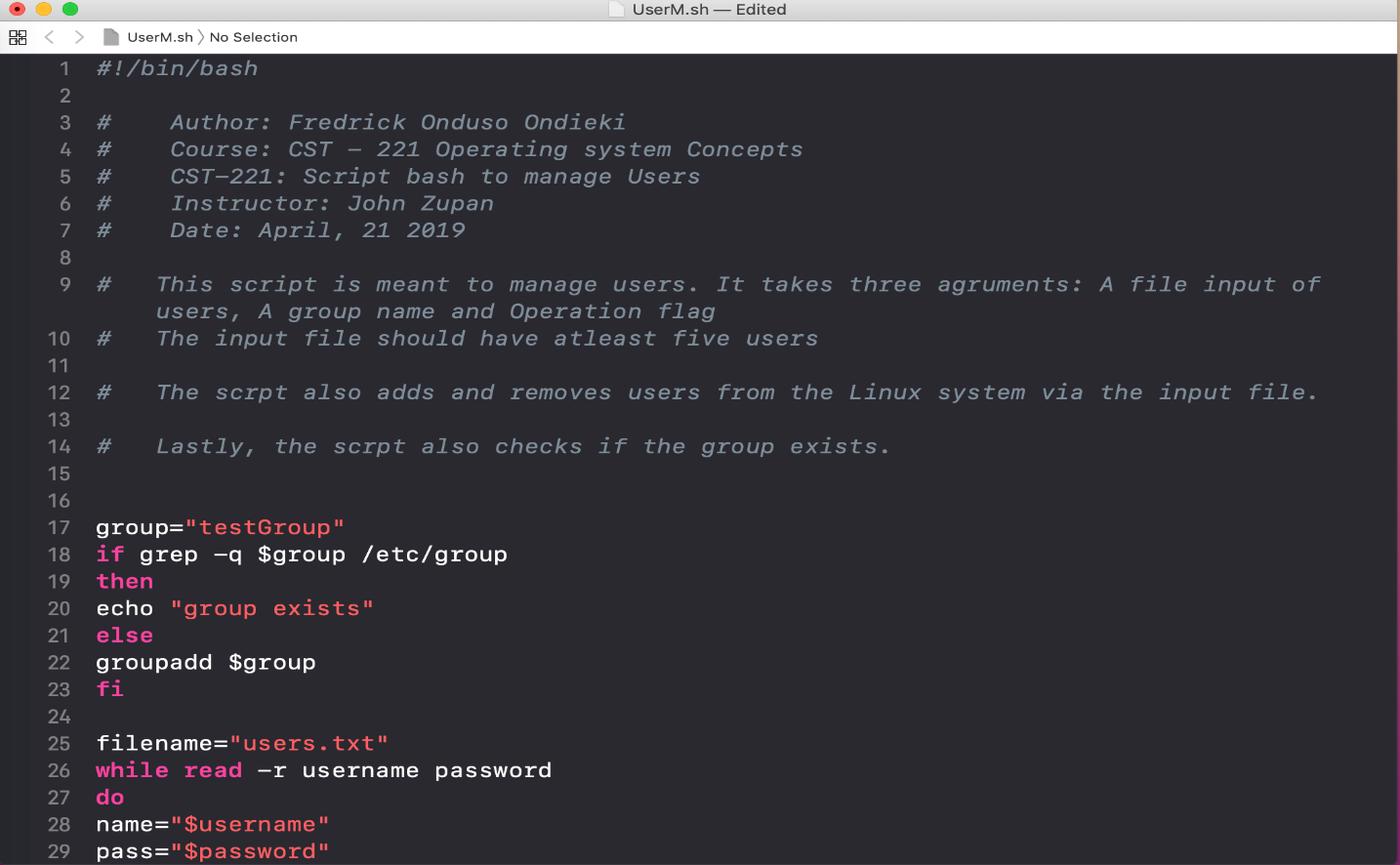


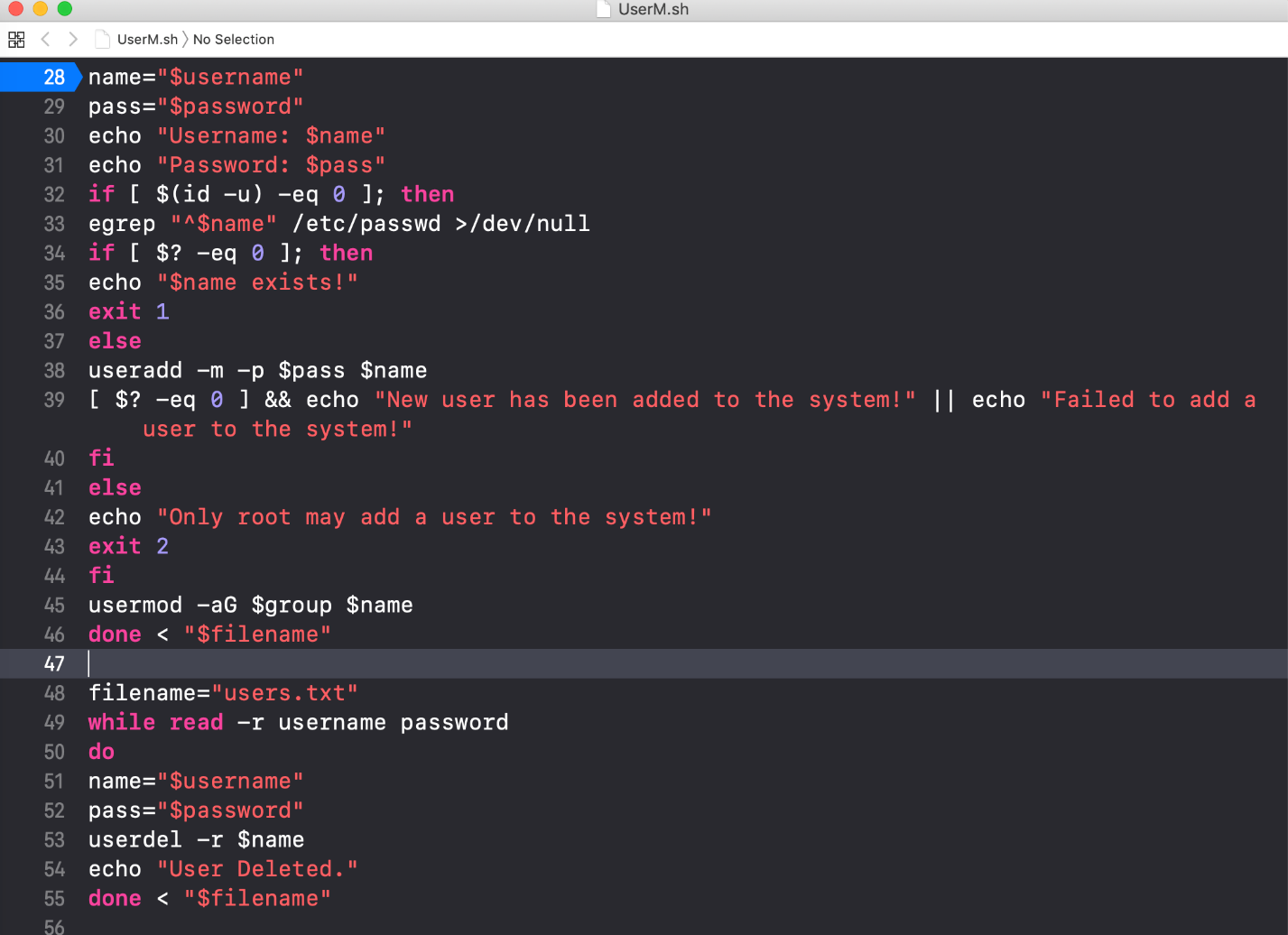




**Bash script to manage users:**

The script will take three script arguments: ***an input filename of users, a group name, and an operation flag.*** The input filename of users to manage will be a text file with a list of users to add to the system or remove from the system. Each line in the file will contain a User ID and an Encrypted Password, which are separated by a space character as a delimiter. Your input user file should have at least five users. 





References

Buffer Overflow. (2019). Retrieved April 16, 2019, from https://www.techopedia.com/definition/2760/buffer-overflow

DevSolar. (2016, February 23). Why are programs written in C and C so frequently vulnerable to overflow attacks? Retrieved April 17, 2019, from https://security.stackexchange.com/questions/115507/why-are-programs-written-in-c-and-c-so-frequently-vulnerable-to-overflow-attac

Perlamo, E. (2013, November 22). What Is a Zero-Day Exploit? Retrieved April 20, 2019, from https://www.tomsguide.com/us/zero-day-exploit-definition,news-17903.html

Penetration Testing Training with Kali Linux. (2019). Retrieved April 20, 2019, from https://www.kali.org/penetration-testing-with-kali-linux/

Love, R. (2013, June 30). How does an operating system detect buffer overflows? Retrieved April 17, 2019, from https://www.quora.com/How-does-an-operating-system-detect-buffer-overflows

Rouse, M., & Cobb, M. (2016). Buffer overflow. Retrieved April 17, 2019, from https://searchsecurity.techtarget.com/definition/buffer-overflow

Tenenbaum, A. S., & Bos, H. (2015). Modern Operating Systems (Fourth ed.). Upper Saddle River, NJ: Pearson Education.

What is Zero-Day Exploit (Attacks)? (2019). Retrieved April 20, 2019, from https://securebox.comodo.com/pos-system/zero-day-attack/

What is a Zero-Day Exploit? Zero-day exploit: An advanced cyber-attack defined. (2019). Retrieved from https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html