**Security**

Mathew Paschall

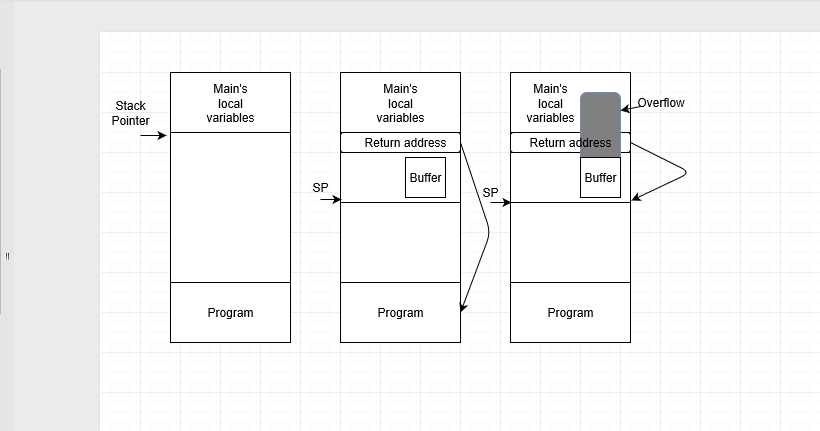
CST-221

John Zupan

March 4, 2018

Buffer Overflow

1. A Buffer Overflow happens when there are too many characters for the buffer to hold. The buffer fills up and then begins overwriting the stack. This causes issues with the system of course.



(Tenenbaum & Bos, 2015)

1. A Buffer Overflow can cause harm to the system by making a program crash or allowing hackers control of the system. This happens because the input is written over some things on the stack, as the input goes outside the buffer that was originally created. If a hacker writes some code outside of the buffer, it can overwrite the stack and give commands to the system, giving them control.
2. A technique that ensures that a Buffer Overflow does not occur is input authentication. Making sure that the input length is below a certain number of characters can thwart many attacks using a Buffer Overflow approach. The operating system reacts to Buffer Overflows with a segmentation fault. This fault happens when a process tries to access memory that is not mapped into its address space (Love, 2013).

Zero Day Exploit

1. A Zero Day Exploit is an exploit that occurs before developers have started working on a patch for the issue. This usually occurs because the developer is not aware that there is an issue until a problem presents itself (Palermo, 2013). Sometimes these exploits can be caused by negligence, or it could be that there is some new way of attacking that the original developers had not foreseen. Attacks using a Zero Day Exploit can be very damaging as hackers have a head start on the developing of updates and can freely do damage until the developers become aware and come up with a solution. Developers should be vigilant when creating their programs to ensure that their programs are as invulnerable to attacks as possible.
2. If a Zero Day Exploit is found, you are the first to know about it, and there is substantial monetary gain to be had, you have a serious ethical decision to make. Do you take advantage of this exploit to make money or report it right away to start fixes. Ethically you should report the exploit to developers with the power to fix it, and ignore the fact that you could benefit from it. You should also not inform anyone besides parties that can fix it, or you risk becoming an accomplice if they decide to exploit it. This ensures that you are being as ethically sound as possible.

Kali Linux

1. Kali Linux is a Linux distribution geared towards ethical hacking and penetration. It comes standard with hundreds of tools to assist in penetrating systems. Kali Linux is made by Offensive Security, who provides a training course that is difficult, but has a highly sought-after certification, OCSP. This training is knowledge based, and you will spend time attempting to penetrate computers in a lab environment to prove your understanding (Penetration Testing Training with Kali Linux, 2018). Kali Linux also provides tools for Computer Forensics, Security Research, and Reverse Engineering. In short, Kali Linux is perfect for anyone who wants to get into the field of ethical hacking, or needs to learn how hackers may attempt to maneuver around security of their programs.
2. Tools.
3. Ethical issues could arise when knowing and using Kali Linux because it will allow you to hack into systems. This could be used for ethical or unethical reasons. If you decided to use Kali Linux with bad intentions to make money, commit fraud, or other reasons, you would be putting yourself in an unethical situation. You should only use Kali Linux to an ethical end. This can include hacking ethically, researching hacking techniques to improve security, or find out what happened if your system or program is hacked. Most things that can be used for good purposes can also be used for bad purposes. Kali leaves the choice up to the user, and we must make the choice to use these for ethical purposes.

References:

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

Love, Robert. June 30, 2013. How does an operating system detect buffer overflows. Retrieved March 4, 2018 from https://www.quora.com/How-does-an-operating-system-detect-buffer-overflows

Palermo, Elizabeth. What is a Zero Day Exploit. November 22, 2013. Retrieved March 4, 2018 from website https://www.tomsguide.com/us/zero-day-exploit-definition,news-17903.html

Penetration Testing Training with Kali Linux. (n.d.). Retrieved March 4, 2018 from website https://www.kali.org/penetration-testing-with-kali-linux/

What is Kali Linux. (n.d.). Retrieved March 4, 2018 from website https://docs.kali.org/introduction/what-is-kali-linux