Security

Daniel R. Cender

Grand Canyon University: CST-221-O500

Feb 20, 2020

This assignment will explore a variety of angles around the topic of security in operating systems.

**Buffer Overflow**

**Explanation**

A buffer overflow is a condition in a program where the attempted memory access exceeds the scope of memory allotted for the program. It’s often exploited as a security vulnerability in large programs based in languages like C/C++ that have little or no automatic memory garbage collection or array bounds checks.

**Diagram**

Figure 1 shows the process of how a buffer overflow can occur.

A close up of a map

Description automatically generated

*Figure 1.* Diagram of how buffer overflow occurs and the result.

**Issues and Harm**

Buffer overflow is, at the very least, a great annoyance to software developers. Programs may crash at the worst moments or behave erratically if buffer overflow cases are not sniffed out in the code and fixed promptly. In regard to security, however, buffer overflow is a massive spot of potential vulnerable which operating systems must vigilantly prevent from occurring. If an attacker can override a function pointer in the memory heap, they could make the program crash, call an unwanted function, or a malicious piece of injected code (Arora, 2013).

**Prevention**

Modern CPUs have a few methods for preventing buffer overflow. One of the most common methods is using pieces of data on the stack, called “stack canaries,” which are checked for changes which will indicate an overflow of allocated address space (Tanenbaum, 2015). This may work for most cases, but highly intelligent attackers can still circumvent stack canaries. Modern operating systems support an “NX” (No-eXecute) bit, dictates that data bits may be written to, and text pieces may be executed (Tanenbaum, 2015). More broadly, this is known as DEP (Data Execution Prevention), which can be enforced in hardware or software (Tanenbaum, 2015). As a developer, it’s imperative to not implicitly trust users to input the information you expect of them. User input should always be checked and cleaned of improper statements.

**Zero Day Exploit**

**Description**

A zero-day exploit is a security vulnerability that originates in a bug produced by a certain software or hardware vendor, which has yet to be patched (Porup, 2019). It’s called a “zero day” vulnerability because that’s exactly how many days a fix has been available for it. These exploits are commonly discovered and then traded around on both “black markets” and “grey markets,” where there is a fuzzy dividing line between which state agencies are allowed to buy or not (Porup, 2019). There are many cases where organizations offer “bug bounties” to those who discover zero day exploits and turn them into the vendor promptly. Unfortunately, a whole other host of organizations drag their feet when alerted to these exploits by private researchers, resulting in greater damage if the exploit ends up discovered and used by a malicious actor first.

**Ethical Issues**

Today, work and vocation are primarily seen as a means towards pure self-fulfillment, self-actuation (Kim, Fisher, & McCalman, 2009). This view prizes material gain and contrasts the values of the more traditional, Christian perspective that work is an encompassment of a person’s God-given purpose to steward resources in diligent service. Zero day exploits certainly seem like a handy way for someone to make quick money, and potentially from multiple parties. A person can go ahead and sell the exploit on a grey or black market (whichever pays highest) and then sell it for a “bug bounty” to the vendor, profiting from multiple angles without consideration to how the black market may use the knowledge. This would be upholding a post-modern view of vocation and use of one’s skillset. On the other hand, someone working from a Biblical perspective would likely be compelled to reveal their findings to the vendor so any bugs can be fixed before the masses are negatively impacted. Although they might stand to gain materially from their technological prowess, it might as well be them one day that will be hurt by a zero-day exploit attack. It’s best for them to treat their fellow computer users as they would like to be treated, by protecting vulnerable devices from exploits they have ready knowledge of.

**Kali Linux**

**Description**

Kali is a Debian-based Linux distribution put out and maintained by Offensive Security today (Everything You Need To Know About Kali Linux, 2019). It is a free operating system packed full of tools useful for network analysts, penetration testers, and ethical hackers. Since it is an open-source project, all of its source code is publicly available, along with the six hundred or so tools it comes installed with. This operating system focuses in on that purpose of security testing, so it’s not a system anyone might expect to be advertised for consumer models of computers, as macOS or Windows are.

**Tools**

Some popular tools that “ship” with Kali are:

* Aircrack-ing: Suite of tools that capture WiFi network packets, export data for further processing, simulate network attacks, test network card capabilities, and test for broken encryption usage (WEP or WPA PSK).
* Nmap: This tool discovers the active hosts on a network by intercepting and evaluating IP packets en-route. It can determine what operating systems are running, what firewalls may be operational, and what applications may be conducting activity on the network.
* THC Hydra: This tool conducts brute-force attacks against various network protocols (HTTP, HTTPS, Telnet, FTP, etc.).

There are many more tools that ship with Kali – too many to list out for this assignment.

**Ethical Issues**

There are some large ethical dilemmas that arise when someone becomes proficient in using the tools that come with Kali. It grants users the ability to find many kinds of network security vulnerabilities, with minimal intimate knowledge of cryptography really. The pervasiveness of moral relativism begs whether a community of Kali users could even decide on what is ethical/unethical use of its toolset. Every person could potentially define morality by practicality, personal fulfillment, societal betterment, Biblical standards, or a multitude of other means and outcomes (Kim, Fisher, & McCalman, 2009). One could learn one or two of these tools, then take them to a local café and sniff out a dozen credit cards, or passwords being used openly on an unsecured network connection. From a Biblical perspective, this would be contrary to how God would have humans treat each other and their belongings. Yet, the fragmentation of society around relativism shows that few people may hold this perspective of using these powerful tools. As a software developer, knowledge of Kali and its tool chest may be useful in granting awareness of glaring vulnerabilities in code we write, which we’d be ignorant to otherwise. This could serve to better stewarding our use of coding abilities and how we approach security for the sake of our users.

**Password Strength Bash Script**

**User Management Bash Script**

References

Arora, H. (2013, June 4). Buffer Overflow Attack Explained with a C Program Example. Retrieved February 21, 2020, from <https://www.thegeekstuff.com/2013/06/buffer-overflow/>

Everything You Need To Know About Kali Linux. (2019, December 20). Retrieved February 21, 2020, from https://www.edureka.co/blog/ethical-hacking-using-kali-linux/

Kim, D., Fisher, D., & McCalman, D. (2009). Modernism, Christianity, and Business Ethics: A Worldview Perspective. *Journal of Business Ethics*, *90*(1), 115–121. https://doi-org.lopes.idm.oclc.org/10.1007/s10551-009-0031-2

Porup, J. M. (2019, July 30). What is a zero day? A powerful but fragile weapon. Retrieved February 21, 2020, from <https://www.csoonline.com/article/3284084/what-is-a-zero-day-a-powerful-but-fragile-weapon.html>

Tanenbaum, A.S. & Bos, H. (2015).*Modern Operating Systems.*Chapter 9.