GRAND CANYON UNIVERSITY

LOPESWRITE FEEDBACK CENTER™

Zachary Chambers
test5

Summary

1211 Words

2% SIMILARITY SCORE
Internet Source 2%
Institution 0%

2 PLAGIARISM ISSUES

28 GRAMMAR ISSUES

Zack Chambers

CST 221

John Zupan

February 10, 2019

Potentially missing comma: 2019 → 2019,

GitHub Link: https://github.com/zchambers3/CST-221/tree/master/Final

Security

Buffer Overflow

Duplicated ph...: Buffer Overfl... → Buffer Overfl...

Buffer overflow is what happens when a program or process attempts to write too much data to the buffer, a segment of computer memory reserved for temporary data storage. The first thing to understand is that at the hardware level the instructions of a computer program and its data are essentially the same. The instructions that make up a computer program are a set of numbers stored in memory locations. The data structures, including variables, buffers, stacks, and arrays are also a set of numbers stored in memory locations. There exist places where instructions and data are either intermingled or adjacent to one another.

Grammatical problem with counta...: much → many

Three successive sentences begin wit...: The

A buffer is just a variable or array of a given size that is used to store data being sent to or received from outside of the program. While in a perfect world the program should always check to see that a block of data will fit in a buffer before copying it there, this is not always the case. Many programmers, programming languages, and library functions fail to check, and blindly copy the entire block of data. This is particularly true of programs written in assembly language, C, and C++.

As a practical example, let's say a program has a 256 byte buffer for user input. Let's also say that a malicious user has sent 512 bytes to that program. A quick check of the data block and the buffer would reveal that there is no way for 512 bytes of data to fit in a 256-byte space. However, let's say that the programmer did not write code to perform that check, and that the programming language and library functions do not check either. The result is that when the program copies 512 bytes into a 256-byte buffer, the first 256 bytes of the data block go into the buffer, and the second 256 bytes of the data block overwrite and replace other variables or code that happened to be adjacent to the buffer. Exactly what gets replaced depends on how the program is arranged in memory, but it is true that a malicious user has managed to replace 256 bytes of program code and program data with values that the attacker has chosen. If the attacker chooses the contents of their data block carefully, they may be able to convince the program to execute some of it as program code. This means that the attacker can run code they wrote, making the program do something malicious. Buffer overflows, along with poor coding still remain two of the biggest application security issues.

Passive voice: it is true that

Zero Day Exploit

A Zero Day Exploit is a way of taking advantage of a defect in computer software in order to allow a user, often a malicious user, to do something they should not be doing. Defects get into computer software because it is mostly written by human beings and human beings make mistakes. Defects can be present in software for years without being noticed because the circumstances under which an actual failure occurs can be subtle and complex.

Missing hyphen: Zero Day → Zero-Day

The term Zero Day describes a defect that was in the software from the very beginning, rather than being introduced as a result of later feature additions or similar changes. Therefore, Day Zero defect sits unnoticed for years until someone identifies the circumstances, such as specific keyboard or mouse actions or peculiar input that would trigger an observable failure.

The set of actions that trigger the software to misbehave are the exploit. The result of exploiting the defect might be to allow a user to log in when they should not, allow a logged-in user to do things they should not, etc. The exploit is sort of like a recipe for causing a visible failure. Day Zero exploits are particularly effective because they take advantage of software that some community has come to trust over a period long period of time.

There is a small subindustry of specialists who make a business of identifying day zero defects and selling their exploit procedures, often to criminal enterprises. People in government are also consumers of zero-day exploits, which they use to create cyberweapons, software designed to illicitly gather intelligence, disrupt enemy procedures, damage enemy equipment, or misuse enemy equipment to cause harm. I believe from a Christian standpoint that if these schemes are meant in a malicious manner then they are acts of someone blatantly committing sin. However, if the acts are not intended to be malicious and help the greater good then I think their actions could be acceptable.

Kali Linux

Kali Linux is nothing but just a specialized Linux Operating System. It is a specialized Operating System that one can do every possible thing with every Linux but you need some effort or you need to get your hands dirty with installation and compiling of tools for making an operating system like Kali Linux, but with Kali Linux you get an already compiled Operating System with specialization in Pen testing and Vulnerability Exploitation.

Please find a list of some of the top 10 tools in Kali Linux below.

· Aircrack-ng: A tool for cracking WEP (WIFI) keys.

· Burp Suite: A tool for testing web application security.

· Hydra: Brute force scheme to access passwords. A parallelized login cracker which supports numerous protocols to attack users.

· John: A tool for offline password cracking.

· Maltego: A tool to obtain a significant amount of information gathering about a prospective target in a single sweep of a domain.

· Metasploit Framework: A tool that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

· Nmap: A port scanning utility/tool. It helps determine whether ports are open or closed. It also helps find out the operating system running on the host or target machine (along with services of ports).

· Owasp-zap: A tool for finding vulnerabilities in web applications.

· Sqlmap: A tool for exploiting SQL Injection Vulnerabilities.

· Wireshark: A tool to analyze Network Protocol.

As with everything in life, balance is key. With great power comes great responsibility. As with most interesting questions, it is almost impossible to give a yes or no answer to a question like "Is hacking a sin?" I know there are plenty of people who like hard and fast rules, so they never have to deal with uncertainty, but God appears to trust our judgement a little more than we ourselves do.

Screenshot for Testing Password Strength

Screenshot User Management Bash Script

References

Redundant phrase: period of time → period

Spelling mistake: subindustry → sub industry

Missing past tense for 'used to....: use → used

Spelling mistake: cyberweapons

Possible wordiness: in a malicious manner

Agreement error: committing

Passive voice: are not intended to be

Statistically detect wrong use ...: then → than

Duplicated phra...: Kali Linux Ka... → Kali Linux

Redundant phrase: some of the → some

Spelling mistake: Aircrack-ng

Possible typo: WIFI → Wi-Fi

Web Content: https://tools.kali.org/password-attacks/hy..

Spelling mistake: parallelized → paralleled

Web Content: https://www.hackers-arise.com/single-po..

Spelling mistake: Maltego → Maltese

obtain (get): obtain → get

Spelling mistake: Metasploit

Spelling mistake: Nmap → Map

Spelling mistake: Owasp-zap

Spelling mistake: Sqlmap → Selma

Spelling mistake: Wireshark → Timeshare

Spelling mistake: judgement → judgment

Emphatic reflexive pronoun: we ourselves

Arora, Himanshu. (2013). Buffer Overflow Attack Explained with a C Program Example. Retrieved from https://www.thegeekstuff.com/2013/06/buffer-overflow/

Arun Nath. (2012). Encrypt a string using openssl command line. Retrieved from https://stackoverflow.com/questions/10106771/encrypt-a-string-using-openssl-command-line

GNU.org. (2018). Conditional Constructs. Retrieved from http://www.gnu.org/software/bash/manual/bashref.html#Conditional-Constructs

Kali.org. (2018). What is Kali Linux? Retrieved from https://docs.kali.org/introduction/what-is-kali-linux

Kerestan, Benjamin. (2017). How to detect, prevent, and mitigate buffer overflow attacks. Retrieved from https://www.synopsys.com/blogs/software-security/detect-prevent-and-mitigate-buffer-overflow-attacks/

Marco. (2012). Read a file line by line assigning the value to a variable. Retrieved from https://stackoverflow.com/questions/10929453/read-a-file-line-by-line-assigning-the-value-to-a-variable

Mlebel. (2013). pipe file line by line into multiple read variables. Retrieved from https://stackoverflow.com/questions/15442220/pipe-file-line-by-line-into-multiple-read-variables

nixCraft. (2007). Linux Shell script to add a user with a password to the system. Retrieved from https://www.cyberciti.biz/tips/howto-write-shell-script-to-add-user.html

Radeanu, Radu. (2013). How to increment a variable in bash? Retrieved from https://askubuntu.com/questions/385528/how-to-increment-a-variable-in-bash

Rouse, Margaret. (2016). Buffer Overflow. Retrieved from http://searchsecurity.techtarget.com/definition/buffer-overflow

Rouse, Margaret. (2018). Zero-Day (Computer). Retrieved from http://searchsecurity.techtarget.com/definition/zero-day-vulnerability

Singh, Shaun. (2017). What are all the benefits of using Kali Linux? Retrieved from https://www.quora.com/What-are-all-the-benefits-of-using-Kali-Linux

Techiwarehouse.com. (2010). IP Sniffing and Spoofing. Retrieved from http://www.techiwarehouse.com/engine/423a5281/IP-Spoofing-and-Sniffing-

Tldp.org. (2018). Catching user input. Retrieved from http://tldp.org/LDP/Bash-Beginners-Guide/html/sect_08_02.html

TLDP.org. (2018). Other Comparison Operators. Retrieved from http://tldp.org/LDP/abs/html/comparison-ops.html

Tutorialspoint. (2018). Kali Linux (all tools pages). Retrieved from https://www.tutorialspoint.com/kali_linux/index.htm

Web.cs.du.edu. (n.d.) Password Cracking. Retrieved from http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html