CST-221 Operation Systems

Joe Leon

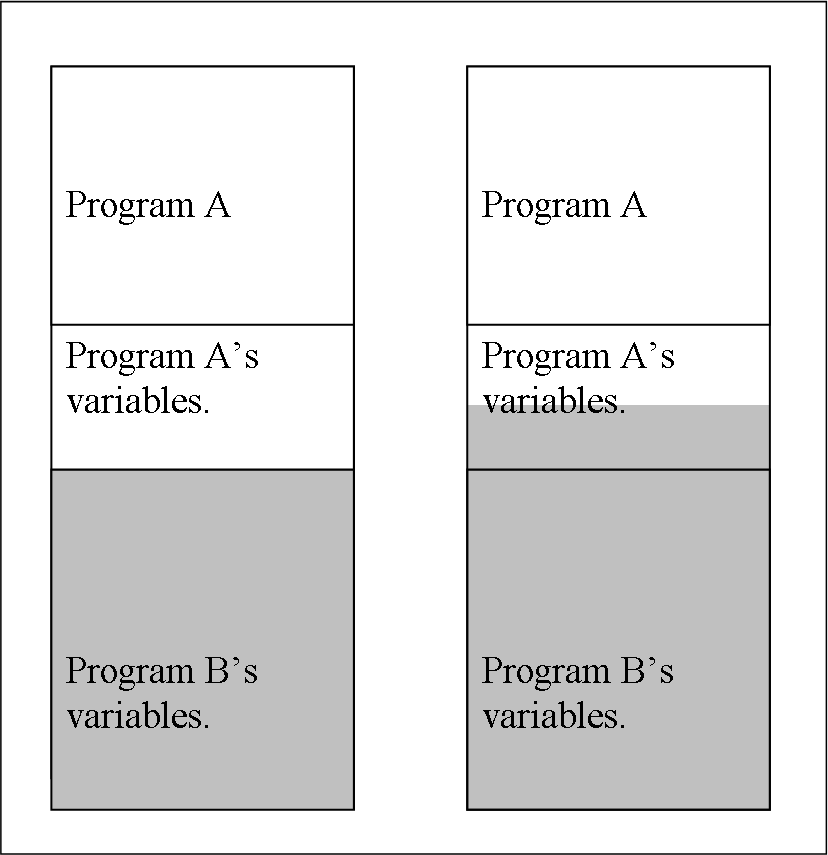
Security

12-24-19

Github link: <https://github.com/SkieXI/CST-221-Final.git>

1a. When a program is running, it request a certain memory size in order to run in which the OS grants. While this program is in use, it will write and rewrite its allotted memory in what is known as a stack. However, in C and C++, there is an oversight where this language does not check the size of the allotted buffer and can write in more information that what that program requested. This can lead to the program to rewrite stacks or block of memory that are used in other programs or even the OS itself. This is what is known as a Buffer Overflow.

1b.



1c. This can be very dangerous as in depending on the information that is written into the buffer and what the buffer spills into, it can affect how other programs are run. This is a very common tactic for running bootleg games on a number of gaming consoles. As poorly written games can leave vulnerabilities in the OS that can be rewritten to ignore security and other credentials to run unauthorized software.

1d. One common technique used to detect if a Buffer Overflow has occurred is to put in a variable at one end of a stack called a Canary Variable. What this does is that periodically, or when that stack’s memory is required, the system will check this variable to see if it has changed or was altered without the system’s permission. This way, the system will know if that stack is safe to run or not.

There are a number of different software out there that are designed to help protect the OS from a Buffer Overflow including a number of libraries that are executed along with the program or are bundled in during its coding phase. As well as it being a feature that a number of anti-virus and malware prevention software provide.

2a. A Zero Day Exploit is a bug or a security hole that has yet to be discovered or patched. This doesn’t mean that no one knows about it. Either the manufacturer of the software has noticed it, but has yet to release a update or a patch, or a hacker or a closed group has discovered this exploit but hasn’t made their discovery public yet. A Zero Day exploit can remain in place for years before a patch is addressed, or when the hacker group makes their move and the exploit is brought to the manufacturer’s or the public’s attention.

2b. From a developer’s point of view, it would be very unethical to discover a exploit or a potential bug, but still ship the product on time or without bringing it to anyone’s attention. Naturally, for any Christian, it would be our duty to bring these oversights to someone’s attention, or take the time and resources to fix it ourselves.

3a. A Kali Linux is a version of the Linux system that is specially designed for OS hardening. This means testing all IO functions and networking functions for security holes or ways to penetrate the OS that the Kali Linux is being tested on.

3b.

|  |  |
| --- | --- |
| Aircrack-ng | Can intercept and monitor any kind of wireless activity within range of the wireless receiver. |
| Ettercap | Monitors and can either modify network activity or prevent it from leaving the system entirely. It can be used as a DOS, (Denial of Service attack) or a DDOS, (Distributed Denial of Service attack.) |
| Burp Suite | A tool used for website testing, encoding, proxy servers, and decoding. |
| John The Ripper | A set of software that is designed to crack passwords. It can either work from a dictionary like system, or just brute force its way in. |
| The Metasploit Project | Security software that can check for remote access as well as any number of OS exploits or vulnerabilities. |
| SQLmap | A database tool that is used to help detect which kinds of SQL injections a database is vulnerable to. It can also detect files that are stored in the database that normal consumers should not be able to access. It can also detect unintended connections. |
| Funkload | A program used to test how much stress a website can handle. This can include data bottlenecks, how many users a server can handle at once, and how well a website can recover after receiving a large work load. |
| Cuckoo | This program can reverse engineer malware and give back some information on how it was built, spread, and what exactly it does. It can also provide a detailed memory and network dump of the contained infected machine. |
| Edb-debugger | The Linux equivalent of the Olly debugger for Windows. Olly is a 32 bit debugger that specializes in finding which registries are called in runtime, which API kits are used, and which libraries and objects are created. |
| Pipal | A tool used to find patterns in use passwords and give a feed back to how vulnerable they are, or more accurately how predictable the passwords are. |
| RouterSploit | A tool used to test how vulnerable a system is when an embedded device is attached to the main computer. |
| HexInject | A packet injector that allows a user to create shell scripts that can read, intercept, and change networking traffic without anyone noticing. |
| SQLdict | A tool used to attack SQL servers through dictionaries. |
| Cisco-torch | Developed alongside Cisco’s “hacking Exposed Cicso Netowrks,” this program can create multiple forks of itself to allows for a much larger scanning process that can still run in the background. It can also discover remote Cisco host. |
| Easside-ng | Allows a user to communicate with other devices without knowing their WEP key. It can determine what the key is, as well as any IP addresses saved to the network. |
| Ivstools | Also included with the aircrack-ng. All it does is merge and convert .ivs files. |
| PadBuster | A Perl script that is used to decrypt ciphertext and plaintext to determine if there is any malice code embedded within a file. Or at least in terms of “padding oracle attacks.” |
| Rptmixsound | A realtime audio editor. It can determine if an audio device such as a mic or a speaker is under attack. |
| Powerfuzzer | An automated web fuzzer, unline other fuzzers, this one was designed to be a lot more user friendly and effective. |
| Shelter | A injection tool, and one of the first dynamic programs to infect a PE. It can only be used in 32 bit applications or frameworks. |
| Smali | Handles Android java VM codes. It can assemble or dissemble dex files and can provide debug information and annotations. |
| Jad | A java decompiler that was specifically designed for java. |
| Wireshark | One of the most popular network protocol analyzer and is even industry standart. It can display any wi-fi usages. |

3c. When it comes to powerful tools that were designed specifically to compromise a computer’s security and expose information and weaknesses, there comes a lot of responsibilities that come along side that. However, these tools in and of themselves are not good or evil, and they could not be discredited simply because of what they are. These tools are very important tools that a lot of companies use in order to find exploits and vulnerabilities to help cover all of their bases.

However, there are going to be those who will use these tools for more malicious intentions. And sadly, even if these tools were not available, there would still be other tools out there that could used instead.