- QUESTION: Find and discuss an example of a buffer overflow exploit. (Minimum word count 300 with references). How could you verify that an overflow condition exists?
- FIELD: COMPUTER SCIENCE

In programming and information security, a buffer overflow exploit or buffer overrun is an anomaly whereby a program writes data to a buffer beyond the buffer's allocated memory, overwriting adjacent memory locations.

According to the free encyclopedia, a buffer overflow occurs when data written to a buffer also corrupts data values in memory addresses adjacent to the destination buffer due to insufficient bounds checking. This can occur when copying data from one buffer to another without first checking that the data fits within the destination buffer. As generally understood, when a software writes more data to a buffer than it can handle, the buffer overflows into neighboring memory, causing a buffer overflow.

Verification on whether a buffer overflow exploit has occurred can be noted by use of Static analyzers, dynamic analyzers and Fuzz testing. Static analyzers examine source code without running it to find potential security holes, while dynamic analyzers evaluate the program during runtime to identify memory-related issues like buffer overflows. Fuzz testing exposes vulnerabilities in a program by introducing random or faulty input.

According to the editorial team's synopsis (February 07, 2017), the best way to prevent buffer overflows when working with source code is to pay close attention to where buffers are used, modified, and accessed. Functions that handle input from users or other external sources should be especially noted, as they would provide the simplest vector for exploitation of the overflow.

The 1988 Morris Worm, which took advantage of a buffer overflow in the finger daemon, is a notorious example of a buffer overflow exploit. The attacker was able to take over Unix systems as a result. According to an investigation conducted by the USA government under the aid of FBI, it was discovered that the worm from Morris only targeted computers running a specific version of the Unix operating system, but it spread widely because it featured multiple vectors of attack. For example, it exploited a backdoor in the Internet's electronic mail system and a bug in the "finger" program that identified network users. It was also designed to stay hidden.

The worm did not damage or destroy files, but it still packed a punch. Vital military and university functions slowed to a crawl. Emails were delayed for days. The network community labored to figure out how the worm worked and how to mitigate it. Some institutions shut down their systems; others disconnected their computers from the network for one week. The exact damages were difficult to quantify, but it's certain to say that the worm created chaos all over and affected normal functioning of the systems.

The incident had a profound effect on a country that was only beginning to realize how vital and vulnerable computers had become. Computer users started to take the concept of cybersecurity more seriously. For instance, the Department of Defense ordered Pittsburgh to establish the nation's first computer emergency response team a few days after the attack. Additionally, developers started producing much-needed software for computer intrusion detection.

A new breed of hackers and a wave of Internet-driven attacks that still affect our digital infrastructure today were both sparked by the Morris Worm at the same time. Whether intentional or not, the nation and the upcoming cyber age were alerted by the first Internet attack, which occurred thirty years ago. This occurrence till today informed the need to improve the online working space to prevent any further attacks.

In conclusion, buffer overflow condition exploit is a serious until today. As demonstrated in this piece of writing, the preventive measures and the suggested solutions should be considered to prevent further setbacks. The Morris worm should serve as a vivid reminder of how serios the exploits can affect people. Verifications on whether the buffer overflow condition has occurred should be conducted early enough using the above suggested techniques. This will aid in early mitigation of the exploits.

REFERENCES

1. **A book with one author**

James C. Forster 2005. Buffer overflow attacks. Published by Syngress ,Rockland, MA.

2. **A book with more than one author and an editor**

(a)Editor: Jason Deckard. Buffer overflow attacks.

(b)Authors: James C. Foster, Vitaly Osipov, Nish Bhalla, Neils Heinen. 1999 Buffer overflow attacks.

3. Synopsis from the Editorial team. February 07, 2017 [online] Available:

https://www.synopsys.com/blogs/software-security/detect-prevent-and-mitigate-buffer-overflow-attacks.html

4.United states government website. November 2, 2018 [online] Available:

Fbi.gov/news/stories/morris.worm.30 years. worm.30years since first major attack on internet. [November 2 ,2018]