BIRZEIT UNIVERSITY

Name: Jumana Abu Murra **Day:Tuesday**

ID:1220594 **Date: 14.feb.2023**

Dr: Asem Kitana **section:2**

Assignment#3

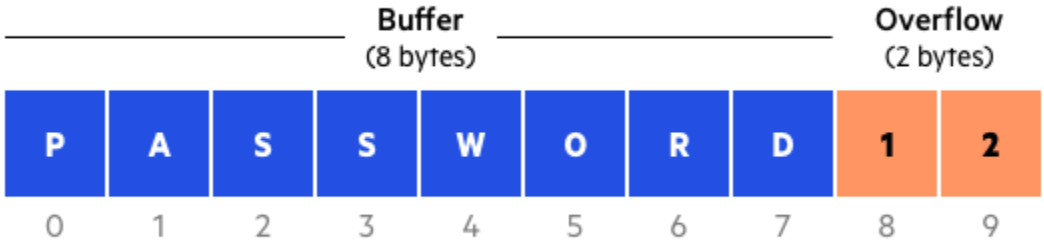
Q1:

One of the buffer overflow attack causes is "Ineffective or lacking of input validation"; explain this cause in details, with mentioning an example that clarify this cause other than the example in the slides.

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write

the excess data past the buffer boundary. Buffer overflows can affect all types of software.



Q2:

Establishing a backup strategy of a particular system could act as a defense mechanism against malware damages (e.g. files deletion). Explain in details this statement, and provide an example.

Having a backup strategy in place can act as a defense mechanism against malware damages, such as file deletion, by providing a way to recover data that has been lost or corrupted. A backup strategy is a set of procedures and technologies used to create and maintain copies of data, so that it can be restored in the event of a data loss or corruption.

For example, consider a company that has important financial data stored on a networked file server. If the server were to be infected with malware that deletes files, the company would face the risk of losing critical data. However, if the company has a backup strategy in place, it could restore the deleted files from the backup, minimizing the impact of the malware attack.

Steps that a typical backup strategy includes:

1) Decide which data should be backed up, such as important files, databases, and application settings.

2) Selecting a backup method, such as full backups, incremental backups, or differential backups, depending on the size and frequency of changes to the data.

3) Selecting a backup location, such as an external hard drive, cloud storage, or a network-attached storage device.

4) Configuring the backup software to run automatically at regular intervals, such as daily or weekly.

5) Regularly testing the backups to ensure that they can be restored successfully in the event of a data loss.

In short, having a backup strategy in place can serve as a defense mechanism against malware damage by providing a way to recover lost or damaged data. It is important for organizations to invest in a backup strategy to ensure that their critical data is protected.

Q3:

There are three main reasons that could facilitate the mechanism of malware installation, list them, and provide an example of each reason that clarifies the concept.

There are three main reasons that can facilitate the mechanism of malware installation:

1) Software loopholes and flaws, example: SQL Injection (SQL injection is a vulnerability that occurs when a software program does not properly validate user-generated data before using it in a database query, allowing an attacker to inject malicious code into the database).

2) Improper system configurations can have serious consequences for the security and stability of a system, example: inadequate password (Using weak passwords, or using the same password for multiple systems, makes it easier for hackers to gain unauthorized access), and Misconfigured servers (Misconfigured servers, such as email or web servers, can be exploited by

attackers to gain unauthorized access to systems or launch attacks against other systems)

3) Luring users to download malicious scripts, example: Drive-by Downloads (Drive-by downloads occur when a user visits a compromised website and a malicious script is automatically downloaded onto their device without their knowledge or consent. This can happen if the website has been hacked and the attacker has inserted the malicious script into the website's code).

Q4:

By using one of the free search engines, search for an example of (other than the ones in the

slides):

Virus, Worm, Trojan, and Rootkit

And explain briefly the operation (e.g. mechanism, targets, and damages) of each example.

I love you

sometimes referred to as Love Bug or Love Letter for you, is a computer worm that infected over ten million Windows personal computers on and after 5 May 2000. It started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs." At the time, Windows computers often hid the latter file extension ("VBS," a type of interpreted file) by default because it is an extension for a file type that Windows knows, leading unwitting users to think it was a normal text file. Opening the attachment activates the Visual Basic script. First, the worm inflicts damage on the local machine, overwriting random files (including Office files and image files; however, it hides MP3 files instead of deleting them), then, it copies itself to all addresses in the Windows Address Book used by Microsoft Outlook, allowing it to spread much faster than any other previous email worm.

you click the attached file called "LOVE-LETTER-FOR-YOU.TXT.VBS" and… nothing seems to happen. However, sometime later, you discover that important documents on your hard disk have been irreparably corrupted, and a bunch of similar love letters have been sent out on your behalf — to all of the contacts in your address book.

'I love You': a computer virus caused $10 billion in damage and exposed vulnerabilities which remain 20 years on.

ILOVEYOU is considered one of the most virulent computer viruses ever created. This virus infected computers through email and appeared as a love confession to the recipient. Once people clicked on the attachment, it immediately sent itself out to everyone in the user's email list, overwrote files, and made the infected computer completely unbootable.

It was catastrophic for large corporations and governments. Having spread among roughly 50 million computers in just 10 days, it caused the CIA, Pentagon, and a host of large corporations to shut down their email systems.