Buffer overflow Attack

Buffer overflow attacks – Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

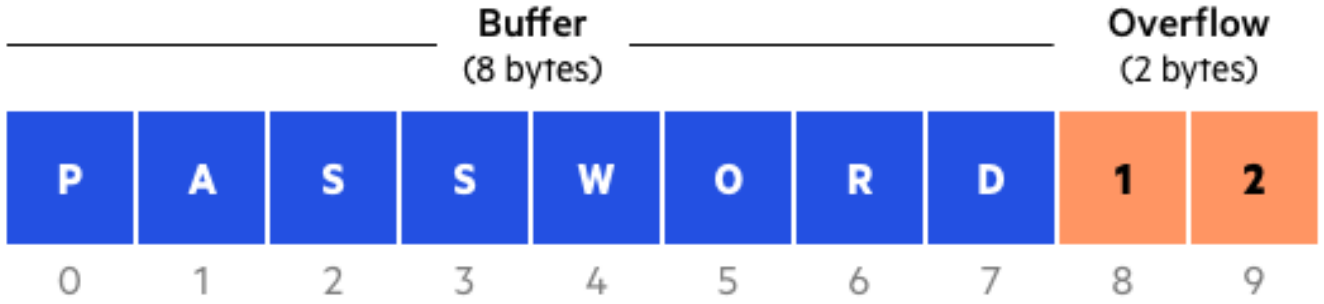
For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

Mitigations:

1. **Address space randomization** - Randomly rearranges the address space locations of key data areas of a process. Buffer overflow attacks generally rely on knowing the exact location of important executable code, randomization of address spaces makes that nearly impossible.

2. **Data execution prevention** - Marks certain areas of memory either executable or non- executable, preventing an exploit from running code found in a non-executable area.



Social Engineering Attack

- Social engineering attacks are a type of cybercrime wherein the attacker fools the target through impersonation.

  They might pretend to be your boss, your supplier, someone from our IT team, or your delivery company. Regardless of who they're impersonating, their motivation is always the same — extracting money or data.

- Social engineering is the art of manipulating people so they give up confidential information

  Criminals usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software

Click on the link to know more: https://www.youtube.com/watch?v=Vo1urF6S4u0

Mitigations

1. NEVER provide confidential information or, for that matter, even non-confidential data and credentials via email, chat messenger, phone or in person to unknown or suspicious sources.
2. BEFORE clicking on links both in emails and on websites keep an eye out for misspellings, @ signs and suspicious sub-domains.
3. Don’t Open mails from untrusted sources
4. Employee Awareness
5. USE 2-factor authentication serrat/12-18

Phishing

- Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need.
- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware or revealing of sensitive information

.***Click on the below Links to view Examples of Phishing attack.***

https://www.phishing.org/phishing-examples

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/best-practices-identifying-and-mitigating-phishing-attacks

Spear Phishing.

Spear phishing is an email scam targeted towards **a specific** individual, organization or business.

Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic.

Spear phishing is often the first step used to penetrate a company's defences and carry out a targeted attack. Attackers use the information they have gathered during reconnaissance to make the email appear personalized.

Whaling & Vishing

Whaling : When attackers go after a “big fish” like a CEO, it’s called whaling.

These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials.

Whaling is of particular concern because high-level executives are able to access a great deal of company information.

Vishing or voice phishing, involves a malicious caller purporting to be from tech support, a government agency or other organization and trying to extract personal information, such as banking or credit card information.

To know more about Vishing click on the below link:

https://www.youtube.com/watch?v=DysFLnOf4Nw

Mitigations for Phishing & its Types:

1. Use Email Security Solutions (to block obvious phishing and spam emails)
2. Educate users
3. Use DMARC (Domain-based Message Authentication, Reporting and Conformance)

---DMARC is a standard for verifying the authenticity of an email. It offers email receivers a way to verify if a message is really from a authorized sender or not.