Unit 4 - Programming language concepts

1. What is ReDOS and what part do 'Evil Regex' play?

A Denial of Service (DoS) attack describes a network attack aiming at making a system inaccessible to its legitimate users (snyk, n.d). The Regular expression Denial of Service (ReDoS) is a Denial of Service attack targeting Regex implementations. A regular expression (regex) is a sequence of text that allows a user to search, locate and edit text (ComputerHope, 2020). While regex is a very powerful tool, when the text input is vast, the regex software works very slowly. This enables an attacker to cause a Regex program to run slowly but introducing a huge amount of input text leading to a sluggish system (Weidman, n.d).

Evil Regex is a long text input that a hacker can introduce to a system and make it vulnerable to DoS attacks. Once the system comes across an Evil Regex it will not realise it is not a legit entry as all parameters are met, however, while the Regex system takes all resources to complete the calculation, the whole system will become slow and vulnerable to external attacks (Patel, 2019).

2. What are the common problems associated with the use of regex? How can these be mitigated?

While regular expressions (Regex) are powerful tools for solving problems, they are difficult to understand and code. Jamie Zawinski, an early Netscape engineer quoted the famous "Now you have two problems". The first problem is the actual problem a user is trying to solve using regular expressions, and the second problem is how to correctly use the Regex program (Friedl, 2006). In comparison to other programming languages, a wrongly coded regular expression will not lead to a failure but will run normally, even though the result will not be the desired. Additionally, it is very easy to produce a wrong regular expression, for example, unbalanced braces will not cause a failure, or different symbols have different meanings in various situations (Larson, 2018).

3. How and why could regex be used as part of a security solution?

Regular Expression is a powerful tool that can search and edit complex text easily. This allows security professionals to review and search multiple files daily. For example, a security professional can run Regex against a log file and search for simple terms, or more accurate results. This includes a simple IP address search, or a search including other metrics (such as hostnames, usernames, etc.) (Li, 2020).

Additionally, Regex can be used to specify firewall rules. This could include blocking requests that contain terms such as rar, exe, tar, etc. (Li, 2020).

References:

ComputerHope (2020) Regex Available from: https://www.computerhope.com/jargon/r/regex.htm [Accessed 01 June 2021].

E. Larson, "[Research Paper] Automatic Checking of Regular Expressions," 2018 IEEE 18th International Working Conference on Source Code Analysis and Manipulation (SCAM), 2018, pp. 225-234, doi: 10.1109/SCAM.2018.00034.

Friedl, J. (2006) Source of the famous “Now you have two problems” quote Available from: http://regex.info/blog/2006-09-15/247 [Accessed 01 June 2021].

Li, V. (2020) Regular Expressions: A Quick Intro for Security Professionals Available from: https://dzone.com/articles/regular-expressions-a-quick-intro-for-security-pro [Accessed 01 June 2021].

Patel, N. (2019) What are Evil Regexes? Available from: https://medium.com/@nitinpatel_20236/what-are-evil-regexes-7b21058c747e [Accessed 01 June 2021].

Snyk (n.d) Regular Expression Denial of Service (ReDoS) Available from: https://snyk.io/vuln/SNYK-JS-SSRI-1246392 [Accessed 01 June 2021].

Weidman, A. (n.d) Regular expression Denial of Service – ReDoS Available from: https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS# [Accessed 01 June 2021].