Definición de diversos ataques de seguridad

Sergio García Prado

October 1, 2016

I. Brute Force: Fuerza Bruta

El ataque por fuerza bruta se basa en la obtención de la clave para acceder a un recurso protegido, ya sea el acceso a un servicio o el descifrado de datos. El método consiste en probar diferentes claves hasta encontrar la correcta. Para ello se suelen utilizar diccionarios de claves más comunes. Este método se suele utilizar cuando no existe otro que pueda aprovechar alguna vulnerabilidad del sistema objetivo. Computacionalmente es muy costoso ya que en el peor caso tendría que probar todas las posibles combinaciones. En muchos casos es fácil protegerse ante este tipo de ataques limitando el número de intentos al introducir la clave.

II. Cache Poisoning: Envenenamiento de Caché

III. DNS Poisoning: Envenenamiento de DNS

IV. Cross-Site Request Forgery (CSRF) o Falsificación de petición en sitios cruzados

V. Cross-Site Scripting (XSS) o Secuencias de comandos en sitios cruzados

VI. Denial of Service (DoS)

VII. LDAP injection

VIII. Man-in-the-middle

IX. Session hijacking attack

X. SQL Injection: Inyección SQL