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

Este tipo de ataque consiste en la substitución del contenido de una determinada cache por otro de carácter malicioso que será servido como si fuera el original. Este ataque normalmente se realiza sobre caches web afectando a todos los usuarios que utilicen dicha cache.

III. DNS Poisoning: Envenenamiento de DNS

El envenenamiento de DNS sigue la misma estrategia que el ataque anterior, sólo que en este caso no se orienta hacia una cache sino hacia un servidor DNS. Con esto se consigue redirigir el tráfico dirigido a un determinado host hacia otro con intenciones poco claras. Generalmente estos destinos simulan el comportamiento que tenía el antiguo servidor pero además tratan de extraer claves u otros recursos valiosos.

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

Este ataque consiste en la inyección o modificación de peticiones realizadas por un host cliente hacia un host servidor. La vulnerabilidad de este ataque se basa en que el host servidor confía en las peticiones realizadadas por el host cliente. La manera más común de ejecución es la modificación de peticiones HTTP como GET o POST Este método es utilizado para casos como modificar la contraseña de un usuario por una conocida o realizar compras sin la autorización del cliente.

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

Este tipo de ataque es el opuesto al anterior: consiste en la ejecución de código no autorizado en el cliente, que se recibe camuflado como si viniera desde un servidor de confianza. La forma más común de introducir el código en el host cliente es la inserción como código JavaScript en páginas web. Este tipo de ataques generalmente pretenden conseguir el robo de información del cliente y como vulnerabilidad utilizan la confianza que este tiene en el host servidor al que está conectado.

VI. Denial of Service (DoS)

El ataque de denegación de servicios consiste en la interrupción de la actividad de un host servidor debido al colapso por una gran afluencia de tráfico dirigido hacia él. Con ello se consigue que los accesos legítimos al recurso no puedan llevarse a cabo debido al colapso por los artificiales. La vulnerabilidad en la que se basa este ataque es la limitación física de procesamiento del host servidor. Este tipo de ataque es muy popular entre hacktivistas.

VII. LDAP injection

Este ataque consiste en la ejecucción de código malicioso en el host servidor generalmente introducido a partir de entradas de formularios web. Lo que se busca generalmente en este tipo de ataques es obtener mayores privilegios para acceder al host servidor o la obtención de información en la respuesta a la petición del formualrio.

VIII. Man-in-the-middle

El ataque Man in the Middle se dirige generalmente a una conexión entre pares (dos hosts) y consiste en la colocación de un tercero entre medias cuya finalidad es obtener y/o modificar el tráfico de datos que pasa a través de él. Una manera de protegerse ante este ataque es mantener una comunicación cifrada eliminando el riesgo a que el tercer host no pueda entender la información ni añadir nueva, aunque si puede eliminarla.

IX. Session hijacking attack

El ataque se basa en la obtención de acceso no autorizado a los recursos de un sitio web mediante la obtención de un token de acceso por cualquier vía, ya sea man-in-the-middle, fuerza bruta, etc. Muchos servicios web utilizan sistemas de token para controlar el acceso a sus recursos, los cuales son entregados al host cliente una vez que se ha autenticado en el servicio. Este ataque por lo tanto realiza una vulneración de identidad sobre un cliente real del servicio para obtener acceso.

X. SQL Injection: Inyección SQL

Este ataque es muy común y consiste en la ejecución de código SQL en una base de datos donde se almacena información valiosa. Estas sentencias generalmente se camuflan entre los campos de un formulario HTTP y se ejecutan en el momento de almacenar dichos valores en la base de datos. Actualmente muchos gestores de base de datos (DBMS) validan la entrada antes de realizar la sentencia para prevenir dichos ataques.