**MINISTERIO DE EDUCACIÓN**

**UNIVERSIDAD TECNOLÓGICA DE PANAMÁ**

**FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES**

**TALLER #6 Y #7**

**CARRERA**

LIC. EN DESARROLLO DE SOTWARE

**ASIGNATURA**

SEGURIDAD INFORMÁTICA

**ESTUDIANTES**

CHRISTOPHER JIMÉNEZ 8-922-2240

JOMEL MCDONALD 3-740-1458

JOSE LUIS RIVERA 20-14-3191

**PROFESORA**

ISABEL LEGUÍAS

**GRUPO**

1LS-241

**AÑO**

2019

**DESARROLLO**

**Parte A. Desarrolle las siguientes preguntas en base al material de vectores de ataque**

1. **¿Qué son los vectores de ataque?**

Son rutas o métodos utilizados para ingresar a los sistemas de información. Son las técnicas que los atacantes utilizan para explotar las vulnerabilidades en las aplicaciones.

1. **¿Defina y explique cada uno de los ataques de denegación de servicio que se dan en la capa de aplicación?**

* Peticiones Legítimas (Legitimate requests): Los ataques DDoS de la capa de aplicación proceden a través de paquetes HTTP legítimos. No hay prácticamente ninguna diferencia entre una solicitud de ataque y una solicitud normal. La única diferencia reside en la intención, y no en el contenido.
* Volumen de tráfico bajo (Low Traffic Volume): contrario a la capa de red DDoS ataques, donde el ancho de banda de la red se convierte en el cuello de botella, en los ataques DDoS de la capa de aplicación, los recursos del servidor se convierten en el cuello de botella. Debido a eso, el servidor se puede reducir utilizando comparativamente menos solicitudes y, por lo tanto, el volumen de tráfico también es bajo.
* Ataques dirigidos (Targeted Strikes): los ataques DDoS de la capa de aplicación son altamente dirigidos. El ataque puede llevarse a cabo en la CPU, base de datos, memoria o conexiones de socket. Un ataque que intente agotar un recurso no afectará a los otros recursos de ninguna manera, pero el sistema en su conjunto no podrá funcionar.
* Resemblance to Flash Crowds: Un flash crowds es un repentino aumenta el tráfico de usuarios legítimos a un sitio web, en la mayoría de los casos debido a algún evento notable o una mega venta en el caso de sitios de comercio electrónico. Un ataque DDoS de la capa de aplicación a menudo se confunde con una multitud repentina porque ambos eventos están asociados con un pico en solicitudes HTTP legítimas a un sitio.

1. **Defina fuga de información**

Las fugas de información son transferencias anormales o no intencionadas de información confidencial al atacante. Una fuga de información abusa de una transferencia de información ilegal, implícita o involuntaria para pasar datos confidenciales al atacante que no debería tener acceso a esos datos.

1. **¿Qué es confused deputy?**

Es un tipo de escalada de privilegios que engaña a un componente para ejecutar una acción sin privilegios con privilegios más altos. Se supone que un componente privilegiado solo usa sus privilegios para una acción benigna. Al establecer cuidadosamente sude entrada, un atacante sin privilegios puede ejecutar involuntariamente una acción privilegiada.

1. **¿Qué es Escalar Privilegios?**

La escalada de privilegios es un aumento no deseado de privilegios. Un ejemplo de escalada de privilegios es obtener ejecución de código arbitrario. A partir del acceso al servicio y restringido a las funciones proporcionadas por el servicio, el atacante pasa a la ejecución de código arbitrario donde tiene acceso completo a todos los archivos, privilegios y llamadas al sistema de ese servicio. Otro ejemplo de escalada de privilegios es un usuario sin privilegios que puede modificar archivos de propiedad exclusiva del administrador, por ejemplo, a través de una configuración incorrecta de la interfaz web.

1. **¿Qué es Ataque Hijacking?**

Un ataque exitoso de Hijacking redirige el flujo de control de la aplicación a una ubicación controlada por el adversario. Este ataque primitivo le da al adversario el control sobre la ejecución del programa y el puntero de instrucción. El secuestro de flujo de control generalmente se logra sobrescribiendo un puntero de código directa o indirectamente.

1. **Defina Inyección de Código**

La inyección de código supone que el atacante puede escribir en una ubicación en el proceso que sea ejecutable. El atacante puede sobrescribir o modificar el código existente en el proceso, reescribiendo las instrucciones parcial o completamente. Corrupciónexistente el código puede permitir que un atacante obtenga la ejecución del código sin secuestrar el flujo de control, ya que una transferencia de flujo de control benigna puede dirigir la ejecución al código controlado por el atacante.

1. **Defina Código Reutilizable**

En lugar de inyectar código, reutiliceel código existente del programa. La idea principal es unir fragmentos de código existentes para ejecutar un nuevo comportamiento arbitrario.

**Parte B. Llene los siguientes espacios en base al material de seguridad en aplicaciones web.**

1. **La autorización** explica el permiso para aquellos que tienen acceso a sus recursos, en otras palabras, lo que puede hacer con esos recursos es como hacer cambios en su cuenta, modificar archivos y tablas de bases de datos.
2. La seguridad debe abordarse en tres niveles: **red, host y solicitud.**
3. El **firewall** permite o bloquea el tráfico en el puerto, monitorea las próximas solicitudes de tráfico y evita ataques conocidos contra nuestros servidores.
4. Las principales amenazas para un servidor web son: creación de perfiles, denegación de servicio, acceso no autorizado, falta de configuración de privilegios, ejecución de código arbitrario, virus, gusanos y caballos de Troya.