Ataques a servidores WEB

Antonio Doncel Campos

Introducción

- Tipos de Ataque
  - SQL Injection
    - Ataque y protección.
  - DoS & DDoS
    - Ataque y protección.
  - Fuerza bruta
    - Ataque y protección.
  - Cross-Site Scripting (XSS Atacks)
    - Ataque y protección.

Tipos de Ataques

- SQL Injection
  - SQL Injection se basa en insertar cadenas infectadas en las consultas SQL de la base de datos
- DoS & DDoS
  - Son intentos de inundar un sitio con solicitudes externas
- Fuerza bruta
  - Intenta “romper” todas las combinaciones posibles de nombre de usuario + contraseña en una página web.
- Cross-Site Scripting (XSS Atacks)
  - Los atacantes utilizan Cross-Site Scripting (XSS) para inyectar scripts maliciosos en lo que serían sitios web inofensivos.

SQL Injection Ataque

1. Primero tenemos que comprobar si el sitio es vulnerable o no.

2. Analizar el tipo de vulnerabilidad de la pagina

3. Usar tus conocimientos en sentencias SQL y tu inteligencia para realizar el ataque.

SQL Injection Protección

- No confiar en la entrada del usuario.
- No utilizar sentencias SQL construidas dinámicamente.
- No utilizar cuentas con privilegios administrativos.
- No proporcionar mayor información de la necesaria.

DoS & DDoS Ataque

- Dos tipos de ataques:

1. Con CMD y el comando ping:
   - ping IP_ATAQUE –t –l TAM_BUFFER

2. Con LOIC:
   - Herramienta de interfaz grafica que realiza una acción parecida a ping con algunas opciones mas.

DoS & DDoS Protección

- Equipos con antivirus actualizados y monitorizar la actividad anómala dentro de nuestra red.
- Contar con infraestructuras flexibles, que puedan proporcionar capacidad on-demand.
- equipos de seguridad especializados que se interpongan entre el atacante y nuestra infraestructura para detener el ataque.

Fuerza Bruta Ataque

- Dos programas distintos en base Linux:
  1. Medusa:
     - Programa, que se encuentra en el repositorio de linux (y si no es libre y publico), completamente por línea de comandos.
  2. Hydra:
     - Programa publico y gratuito como el anterior que cuenta con una UI para guardar configuraciones de ataques o línea de comandos para realizar un solo ataque.

Fuerza Bruta Protección

- Evitando ataques de fuerza bruta a contraseñas o usuarios (sin conexión)
- Evitando ataques de fuerza bruta a sistemas o servicios (con conexión)
- Bloqueo por IP
- Bloqueo de usuario/contraseña
- Captchas

Cross-Site Scripting (XSS Attacks) Ataque

1. Primero tenemos que comprobar si el sitio es vulnerable o no (mas fácil que SQLI pero mas difícil saber el grado de esta).

2. Analizar el tipo de vulnerabilidad de la pagina

3. Ataque:
   - Cookie Stealing/Logging
   - DEFACING
   - ONMOUSEOVER
   - Hex Bypassing
   - Case-Sensitive Bypassing

Cross-Site Scripting (XSS Attacks) Protección

- Servidores:
  - Limitar los caracteres de entrada
  - Sanear los datos
  - «Escapar» los datos
- Usuarios:
  - Contar con una solución de seguridad instalada y actualizada.
  - Mirar la dirección URL a la que se está accediendo.
  - Utilizar navegadores alternativos, quizás no tan populares, como Opera, Comodo o Chromium.

Conclusión

- No te fíes de ningún sitio web ni de los usuarios que entran en su web.
- Mucha seguridad nunca es suficiente.
- Todos somos el objetivo de los hackers, la información es dinero.