https://github.com/grafov/hulk

El ataque HULK (HTTP Unbearable Load King) es una herramienta para realizar ataques de denegación de servicio (DoS) en servidores web. HULK genera una gran cantidad de solicitudes HTTP únicas y legítimas, con el objetivo de sobrecargar el servidor y hacerlo inaccesible para los usuarios legítimos.

**Características del Ataque HULK:**

1. **Solicitudes Únicas**: HULK genera solicitudes HTTP únicas con parámetros aleatorios en cada solicitud, lo que dificulta que las medidas de mitigación basadas en firmas o patrones detecten y bloqueen el ataque.
2. **Generación de Tráfico Masivo**: El objetivo de HULK es generar una cantidad masiva de tráfico HTTP para agotar los recursos del servidor web, como el ancho de banda, la capacidad de procesamiento y las conexiones disponibles.
3. **Encabezados Aleatorios**: HULK puede modificar los encabezados HTTP en cada solicitud para hacerlas parecer legítimas y evadir los sistemas de detección de intrusos (IDS) o firewalls de aplicaciones web (WAF).

**Cómo Funciona HULK:**

1. **Inundación de Solicitudes**: El atacante ejecuta HULK para enviar una gran cantidad de solicitudes HTTP al servidor objetivo.
2. **Parámetros Aleatorios**: HULK genera solicitudes con parámetros y rutas aleatorias para evitar ser bloqueado fácilmente por reglas de filtrado estáticas.
3. **Consumo de Recursos**: La gran cantidad de solicitudes sobrecarga el servidor web, consumiendo sus recursos y haciendo que el sitio web sea inaccesible para los usuarios legítimos.

**Ejemplo de Uso de HULK:**

Para ejecutar HULK, necesitas tener Python instalado. Aquí hay un ejemplo de cómo ejecutar HULK:

1. Descarga HULK desde el repositorio de GitHub:

bash

Copy code

git clone https://github.com/grafov/hulk.git

1. Navega al directorio de HULK:

bash

Copy code

cd hulk

1. Ejecuta HULK especificando la URL del objetivo:

bash

Copy code

python hulk.py http://www.ejemplo.com

**Medidas de Mitigación:**

Para protegerte contra ataques HULK y otros ataques DoS, considera implementar las siguientes medidas:

* **Limitación de Tasa (Rate Limiting)**: Configura limitaciones de tasa en el servidor web para restringir la cantidad de solicitudes que una dirección IP puede hacer en un período de tiempo determinado.
* **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)**: Utiliza IDS/IPS para detectar y bloquear tráfico sospechoso antes de que llegue al servidor web.
* **Firewall de Aplicaciones Web (WAF)**: Implementa un WAF para filtrar y bloquear solicitudes maliciosas basadas en patrones de comportamiento.
* **Red de Entrega de Contenido (CDN)**: Utiliza una CDN para distribuir el tráfico entrante y mitigar los efectos de un ataque DoS al distribuir la carga entre múltiples servidores.
* **Servicios Anti-DDoS**: Contrata servicios especializados en protección contra DDoS que puedan filtrar el tráfico malicioso antes de que llegue a tu servidor.

Implementar estas medidas puede ayudar a proteger tu servidor web contra ataques de denegación de servicio y mantener la disponibilidad para los usuarios legítimos.