Ataque de Spoofing y DoS al Servidor de WordPress

Resumen del Ataque de Spoofing y DoS

Durante el ejercicio, simulamos un ataque de **Spoofing** y **Denegación de Servicio (DoS)** contra un servidor de WordPress. El objetivo era sobrecargar el servidor con solicitudes falsas y observar su comportamiento.

- **Spoofing**: En este ataque, el atacante oculta su dirección IP real, pretendiendo ser otra persona. Esto hace que sea más difícil rastrear y bloquear el tráfico malicioso.
- **DoS**: El ataque consistió en inundar el servidor de WordPress con solicitudes, lo que provocó que se volviera más lento o incluso inaccesible para los usuarios legítimos.

Monitoreo del Ataque

Usamos herramientas como `htop` en **Kali Linux** para observar cómo respondía el servidor:

- **Uso de CPU**: La CPU del servidor aumentó significativamente, con el núcleo 0 alcanzando más del 80% de uso.
- **Memoria y Red**: El tráfico de red y el uso de memoria aumentaron debido a la gran cantidad de solicitudes que el servidor estaba manejando.
- **Respuesta del Servidor**: El sitio de WordPress se volvió lento y, finalmente, dejó de responder, generando mensajes de error y tiempos de espera para los usuarios reales.

Estrategias para Defenderse de los Ataques de Spoofing y DoS

Para proteger un servidor de WordPress de este tipo de ataques, se pueden aplicar varias estrategias:

1. **Cortafuegos (Firewalls)**:
    - Un **cortafuegos** puede bloquear el tráfico sospechoso o las direcciones IP que envían demasiadas solicitudes.
    - El **limitado de tasas (rate limiting)** ayuda a detener a una sola dirección IP para que no sobrecargue el servidor.
2. **Filtrado de IPs y Bloqueo de Tráfico Falsificado**:
    - Usar reglas de firewall para detectar y bloquear el tráfico con direcciones IP falsificadas.
3. **Balanceo de Carga**:
    - Los **balanceadores de carga** distribuyen el tráfico entre varios servidores, evitando que un solo servidor se vea sobrecargado.
    - Esto también previene que el servidor colapse durante un ataque.

4. **Herramientas de Monitoreo**:
    - Herramientas como `htop` ayudan a detectar picos inusuales en el tráfico y la carga del servidor, lo que permite actuar antes de que el servidor deje de funcionar.

Buenas Prácticas para la Seguridad en WordPress

Para evitar estos tipos de ataques en el futuro, es importante seguir algunas buenas prácticas de seguridad:

- **Actualizar Regularmente**: Mantén WordPress, los plugins y el software del servidor actualizados para evitar vulnerabilidades conocidas.
- **Usar Autenticación Segura**: Implementa contraseñas fuertes y autenticación de dos factores (2FA) para evitar accesos no autorizados.
- **Realizar Copias de Seguridad Regulares**: Tener copias de seguridad recientes te permitirá recuperarte rápidamente en caso de un ataque.