ACTIVIDAD 2 - CONSULTA ZONA DE TRANSFERENCIA EN SERVICIOS DNS

Presentado Por: Pablo Andrés Briceño

1. ¿Qué Es?

Las Transferencias de zona DNS, a veces llamadas AXFR por el tipo de solicitud, es un tipo de transacción de DNS. Es uno de varios mecanismos disponibles para administradores para replicar bases de datos DNS a través de un conjunto de servidores DNS.1 La transferencia puede hacerse de dos formas: completa (AXFR)2 o incremental (IXFR es el mecanismo por el cual un servidor DNS primario suministra información a otro servidor DNS secundario. Si un atacante consigue realizar esta transferencia de zona podría obtener el listado de los servidores internos de una red.

Para entender bien, una transferencia de zona (RFC 5936) es un tipo de transacción DNS (sistema de nombres de dominio, el cual traduce y/o apunta cada dominio a la IP correspondiente) normalmente inducida a través de una consulta tipo “AXFR” para poder replicar bases de datos con registros entre servidores DNS.

La información contenida en cada transferencia de zona puede entregarnos la información de todos los dominios y/o servidores de cada base de datos de registros en el servidor DNS, lo cual puede llevar a fugas de información importantes, especialmente en la parte de reconocimiento de un ataque, es importante limitar o restringir la transferencia de zonas ya que este mecanismo permite a un atacante recolectar información importante.

2. ¿Para Que Sirve?

Sirve para mantener consistencia entre dos o más servidores DNS ósea generar concordancia entre un registro DNS en un servidor “primípara” y “secundarios” estos se actualizan consultando cambios al servidor.