OBSERVATORIO DEL DNS

Autor: Hugo Salgado – NIC Chile <hsalgado@nic.cl>
Versión 0.1, 2/12/2014

Descripción:

El proyecto de Observatorio Latinoamericano del DNS consiste en establecer un punto de medición de parámetros técnicos del protocolo del Sistema de Nombres de Dominio "DNS" con el fin de mejorar el conocimiento de esta tecnología crítica, medir la implantación de nuevas mejoras y cumplimiento de estándares, y establecer buenas prácticas en la configuración y operación del DNS en nuestra región.

Se trabajará sobre la base de tener parámetros técnicos rigurosos y hacer mediciones activas desde distintos puntos de Internet dentro de la región. Es importante notar que se tiene como objetivo en un comienzo la medición de servidores "autoritativos" y no "recursivos".

Como resultado se realizará informes anónimos y agregados de toda la región, además de tener la posibilidad de entregar informes privados dentro de los países que lo soliciten.

Requisitos:

Tener al menos 1 punto de medición activa que disponga de lista de dominios. Es esperado que los TLDs que aporten a esta iniciativa entreguen sus zonas en algún formato privado y seguro. Desde ahí se realizarán las consultas por cada nombre de dominio.

También es posible obtener listas parciales de dominios por otros medios, como el ranking de Alexa por país.

En recursos de hardware basta con 1 servidor con capacidad de realizar consultas masivas, con recursos propios de IPv4 e IPv6. Se debe disponer de un pequeño sitio web con descripción de las mediciones y reporte de abusos o problemas, para informar en caso de caer en bloqueos o IDSs, que se puede mantener en el mismo hardware.

En personal humano se requiere:

Etapa de diseño de pruebas:
- 1 Ingeniero para diseño de pruebas,
- 1 Programador para construcción de pruebas,

Etapa de recolección de datos:
- 1 Técnico para operar y mantener las pruebas,

1 Sysadmin para labores de administración del servidor

Etapa de análisis:

1 Analista para procesar datos

1 Ingeniero para creación de Informe final con conclusiones y recomendaciones.

Es importante notar que estas etapas son cíclicas, porque la recolección de datos es importante repetirlas durante el tiempo; y la misma etapa de análisis más el feedback de la comunidad alimentará continuamente la necesidad de nuevas pruebas.

Estas labores no son de jornada completa ni simultánea, por lo que podrían agruparse algunas de ellas en la misma persona.

Algunas métricas:

1. Número de servidores DNS por cada dominio.
2. Número y diversidad de ASN por DNS de dominio.
3. Dispersión de segmentos IP por DNS de dominio
4. Estado de sanidad de servidores DNS
    4.1 Soporte de estándares mínimos (EDNS, consultas incorrectas, TCP)
    4.2. Métricas de seguridad (puertos variables, no recursividad, etc.)
5. Penetración de IPv6 y DNSSEC
6. Fingerprint de servidores.

Privacidad:

Debido a restricciones de privacidad en cada país, el listado de dominios de un TLD puede considerarse un datos privado y sensible. En este caso habría que firmar un compromiso de buen uso de la información, solo para fines de investigación, y no divulgar ni la lista de dominios ni los resultados en detalle que pudieran dar indicios. Solo pueden divulgarse en forma pública los resultados agregados de toda la región.

Resultados:

Publicación de reportes con gráficos y análisis al menos 1 vez al año, en forma recurrente y usando las mismas métricas, con el fin de comparar la evolución de resultados. Esto permite ver evolución en el tiempo de implantación de nuevas tecnologías, así como medir resultados de ciertas políticas de mejora y cambio.

Además se puede realizar presentaciones en foros y conferencias de la región,

para alimentar la discusión y feedback entre operadores DNS.

Cada TLD que entregue su lista de dominios puede solicitar si lo requiere los mismos resultados para su propio país, en forma privada.