Análisis Comparativo de la Exposición de Servicios Digitales en los Sistemas Autónomos (ASNs) de Bogotá, Basado en Datos Públicos de Escaneo de Internet

Juan Manuel Serrano Rodríguez
Código: 20211020091
Facultad de Ingeniería
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia
jmserranor@correo.udistrital.edu.co

I. FORMULACIÓN DEL PROBLEMA

La infraestructura de internet de Bogotá es un ecosistema complejo, sostenido por múltiples Sistemas Autónomos (ASNs) pertenecientes a proveedores de servicios (ISPs), universidades y grandes corporaciones. La configuración y el mantenimiento de los miles de dispositivos dentro de estas redes determinan su ”higiene digital” colectiva. La exposición innecesaria de servicios —como bases de datos, paneles de acceso remoto o protocolos de comunicación obsoletos— crea una superficie de ataque que puede ser explotada por actores maliciosos, resultando en brechas de datos y disrupción de servicios que afectan a miles de ciudadanos y empresas.

Actualmente, no existe un benchmark o un estudio comparativo público, basado en datos empíricos a gran escala, que evalúe la postura de seguridad de estos ASNs clave para Bogotá. Se desconoce qué redes presentan una mayor concentración de configuraciones riesgosas y cuáles son los patrones de exposición más comunes. Sin esta información, los esfuerzos para mejorar la seguridad digital de la ciudad carecen de un diagnóstico claro y priorizado.

Este proyecto propone llenar ese vacío mediante el análisis de los conjuntos de datos públicos de escaneo de internet de Censys. En lugar de depender de APIs restringidas, se utilizará la plataforma Google BigQuery para consultar estos datos masivos, partiendo de una lista autoritaria de ASNs relevantes para Bogotá identificados a través de LACNIC. El objetivo es crear un informe cuantitativo y reproducible de la exposición digital de la infraestructura de red de la ciudad.

II. OBJETIVOS ESPECÍFICOS

A. Objetivo 1: Identificación y Caracterización de la Exposición por ASN

Realizar un análisis de dos fases para identificar y cuantificar los servicios expuestos en las redes más importantes de Bogotá:

Identificación de ASNs: Utilizar la base de datos pública de LACNIC (Registro de Direcciones de Internet de América Latina y el Caribe) para identificar y documentar los números de Sistema Autónomo (ASN) de los principales ISPs y entidades académicas que operan en Bogotá.

Caracterización de Servicios: Ejecutar consultas SQL sobre los conjuntos de datos públicos de Censys en Google BigQuery para analizar los ASNs identificados, cuantificando la prevalencia de:

- Protocolos de texto plano y obsoletos (Telnet, FTP).
- Servicios de bases de datos expuestas (MongoDB, Redis, MySQL, Elasticsearch).
- Paneles de control de acceso remoto (RDP, VNC).
- Dispositivos de infraestructura con interfaces de gestión públicas (ej. routers con HTTP/HTTPS).

B. Objetivo 2: Desarrollo de un Modelo Cuantitativo de Puntuación de Higiene Digital

Diseñar un modelo de puntuación que permita evaluar y comparar la postura de seguridad de cada ASN de forma objetiva. El modelo:

- Asignará un factor de riesgo a cada tipo de servicio expuesto, considerando la probabilidad de explotación y el impacto potencial (ej. un RDP expuesto tiene un riesgo mayor que un FTP).
- Normalizará los resultados en función del tamaño del espacio de direcciones IP del ASN para permitir una comparación justa entre redes de diferente escala.
- Calculará una ”Puntuación de Higiene Digital” final para cada ASN, clasificándolos para facilitar la identificación de aquellos con mayor área de mejora.

C. Objetivo 3: Implementación de un Dashboard de Inteligencia de Amenazas Públicas

Desarrollar una aplicación web (dashboard) para presentar los resultados de forma clara e interactiva. La plataforma no requerirá inicio de sesión y visualizará los datos agregados:

- Mostrará un ranking de los ASNs analizados según su Puntuación de Higiene Digital.

- Presentará gráficos estadísticos sobre los servicios inseguros más comunes encontrados en toda la infraestructura de Bogotá.
- Permitirá filtrar y explorar los resultados por ASN específico, para ver en detalle su perfil de exposición.
- Incluirá una sección educativa que explique los riesgos asociados a cada servicio expuesto y ofrezca recomendaciones generales para mitigarlos.

III. RESULTADOS ESPERADOS

A. Resultado Principal: Observatorio Público de la Higiene Digital de Redes en Bogotá

Una plataforma web analítica y estática (actualizada periódicamente) que sirva como una fuente de información pública, presentando:

- **Ranking de ASNs:** Una tabla comparativa que clasifica los principales proveedores y redes de Bogotá por su postura de seguridad, basada en datos cuantificables.
- **Perfil de Riesgo de la Ciudad:** Estadísticas agregadas que respondan a preguntas como: ¿Cuál es el protocolo inseguro más común en Bogotá? ¿Cuántas bases de datos están potencialmente expuestas?
- **Visualización de Datos:** Gráficos interactivos que muestren la distribución geográfica de los ASNs con riesgos críticos.

B. Resultado Secundario: Manual Metodológico para Análisis de Exposición Digital

Un documento técnico que detalla el proceso de análisis, incluyendo:

- Descripción del método de recolección de datos (Censys, LACNIC, Google BigQuery).
- Procedimiento para la asignación de puntuaciones de riesgo.
- Herramientas y software utilizados (Python, Pandas, Matplotlib, Flask).
- Recomendaciones para la implementación de medidas de seguridad en redes de Bogotá.
- Descripción del método de recolección de datos (Censys, LACNIC, Google BigQuery).
- Procedimiento para la asignación de puntuaciones de riesgo.
- Herramientas y software utilizados (Python, Pandas, Matplotlib, Flask).
- Recomendaciones para la implementación de medidas de seguridad en redes de Bogotá.

IV. REFERENCIAS

REFERENCES

[1] Censys. `https://www.censys.io/`.
[2] LACNIC. `https://www.lacnic.net/`.
[3] Google BigQuery. `https://cloud.google.com/bigquery`.
[4] IEEEtran document class. `https://www.ctan.org/pkg/IEEEtran`.