Agustín Pumarejo Ontañón A01028997
Adriana Abella Kuri A01329591

Reto 5 - Reporte

A: paul.reto.com (172.23.97.22)
B: kcsi9jgefgh3rfsjmv6l.com (213.193.6.183)
C: fandom.com (215.109.221.174)

1. Utilizando un grafo con las conexiones entre las ip de la red interna, determina la cantidad de computadoras con las que se ha conectado A por día. ¿Es el vértice que más conexiones salientes hacia la red interna tiene?

   Sí, se conecta con 254 computadoras mientras que la segunda computadora interna con más conexiones solo tiene 2.

2. Utilizando el grafo del punto anterior, ubica la cantidad de computadoras que se han conectado hacía A por día. ¿Existen conexiones de las demás computadoras hacia A?

   Sí existen conexiones de las demás computadoras hacia A. En total, 29 computadoras internas se conectan a ella.

3. Utilizando un grafo de conexiones a sitios web, determina cuántas computadoras se han conectado a B por día.

   Solo 1, la computadora A.

4. Utilizando el mismo grafo del punto anterior, indica cuántas computadoras se han conectado a C por día.

   10-08-2020: 5
   11-08-2020: 9
   12-08-2020: 10
   13-08-2020: 10
   14-08-2020: 8
   17-08-2020: 8
   18-08-2020: 12
   19-08-2020: 10
   20-08-2020: 29
   21-08-2020: 7

   Todos los días hubo conexiones 12 computadoras o menos, con la excepción de que el día 20 de agosto se conectaron 29. Este es el mismo día en el que esta dirección tuvo una cantidad anormal de tráfico, con 576 conexiones entrantes.

5. (Pregunta sin código): Investiga que es un ping sweep, un DDoS, un servidor de comando y control y un botmaster. ¿Ves estos elementos en tus datos?

   Ping sweep: Es una técnica que utiliza IPs para averiguar si un grupo de computadoras dentro de la misma red están activas y así saber si pueden ser infectadas.

   DDoS: Un ataque DDoS es un ataque por denegación de servicio. En este ataque se mandan muchas solicitudes desde varios puntos de la red para saturarla e impedir el tráfico normal en ella.

   Servidor de comando y control: Es una computadora que controla a otro grupo de computadoras infectadas con malware. Esta computadora puede ser usada por el operador del malware o puede ser otra computadora infectada.

   Botmaster: Es cuando una persona (el botmaster) controla un grupo de botnets para atacar una red. Una botnet es una red de robots, y los botmasters las usan para hacer ataques DDoS u otros tipos de ataques.

   Sí se ven todos los elementos en los datos. El ping sweep es la conexión entre paul.reto.com (A) y todos los demás usuarios de la red interna. El DDoS es cuando aumenta el número de conexiones a Fandom (B). El servidor de comando y control es paul.reto.com ya que se conecta al resto de las computadoras. El Botmaster podría ser cualquiera de las dos redes sospechosas (B), probablemente es 9kmiofxfryfxdyoypub1.com.

   Bibliografía

   Cloudlare. (2020). Attention Required! Cloudflare. Noviembre 26, 2020, de https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

   Fernández, L. (2020). *Command-and-Control: tu red podría estar bajo control de los cibercriminales*. Redes Zone. Extraído el 26 de noviembre, 2020. URL: https://www.redeszone.net/tutoriales/seguridad/ataques-command-and-control/

   Rouse, M. (2005). *Ping sweep (ICMP sweep)*. TechTarget. Extraído el 26 de noviembre, 2020. URL: https://searchnetworking.techtarget.com/definition/ping-sweep-ICMP-sweep