Reto 5

Carolina Ortega Barrios

A01025254

Ximena Gonzalez Ibarra

A01028604

Escuela de Ingeniería, Instituto Tecnológico de Estudios

Superiores de Monterrey, México, México,Campus Santa Fe

Fecha de entrega : Jueves 26 de noviembre de 2020

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?

La cantidad de computadoras que encontramos que se conectan con A es de 254.

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, existe una computadora conectada a A.

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

Sí existe la conexión a B, pero solo de una computadora.

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

Utilizando el mismo grafo, encontramos que 32 computadoras tienen conexión a C.

```
Compus con las que A se ha conectado: 254
Compus que se conectan a A: 1
Compus que se conectan a B: 1
Compus que se conectan a C: 32
```

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: Se le conoce también como ICMP sweep ó ping scan, es una técnica de escaneo de red que se puede utilizar para averiguar qué direcciones IP se asignan a hosts activos. Un ping sweep usa “Internet Control Message Protocol” que son como peticiones para comunicarse con muchos hosts al mismo tiempo.

Se debe recorrer el archivo de las conexiones entrantes y salientes, de ahí llenamos y buscamos en el grafo cierta información estamos haciendo un “escaneo” de los datos al buscar las conexiones de las ip internas que necesitamos.

Servidor de comando y control: Computador que da órdenes y recibe información de dispositivos infectados con malwares el dispositivo que da órdenes a las computadoras infectadas (hackeadas).

La ip “172.27.197.23” es la ip infectada que se conecta a las demás computadoras. Los ataques hacia el servidor pueden ocasionar hackeos.

DDoS(Distributed Denial of Service): El DDoS(“ataque distribuido denegación de servicio”) es un tipo de ataque en el cual se ataca una computadora con muchos servidores para que este deje de funcionar.

Se ataca a la página “theguardian.com” saturándola con un número de

entradas anormalmente alto en un día.

Botmaster: Se encarga de coordinar los ataques.

En este reto se ve como la computadora que coordina los ataques es la computadora con terminación “.23”. Esta ip se comunica a las otras computadoras de la empresa.

Referencias

N.A. (N.D). “Ping Sweep” Solarwinds.Recuperado de[Sitio web]: https://www.solarwinds.com/es/engineers-toolset/use-cases/ping-sweep

SSD. (N.D). “Servidor de comando y control”. 25 de noviembre 2020, [Sitio web]: https://ssd.eff.org/es/glossary/servidor-de-control-y-comando

Julian, G. (2016). “¿Qué es un ataque DDoS, cómo pararlo?” [Sitio web]: https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta

Leonardo(N.D) “¿Qué es un botmaster?” Botifica.Recuperado de[Sitio web]: https://botifica.com/blog/que-es-un-botmaster/