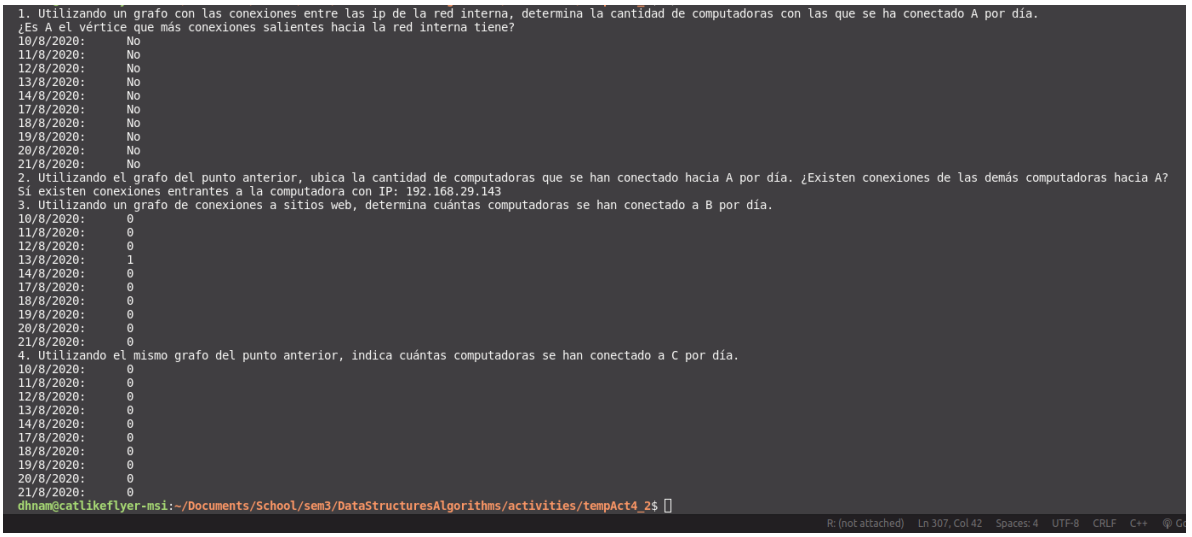
Emiliano Cabrera - A01025453
Do Hyun Nam - A01025276

Investigación Act-4.2

Programa



Conceptos

Un ping sweep (o barrido de puertos) es un ataque que envía peticiones “ping” a un rango de direcciones IP, teniendo como objetivo el encontrar hosts y probarlos en busca de vulnerabilidades. (*Ping Sweep*, n.d.)

Un DDoS (ataque de denegación distribuida de servicio) es un tipo de ataque que aprovecha los límites de capacidad que tiene un recurso de red. El DDoS envía múltiples solicitudes al recurso atacado, con la intención de desbordar su capacidad y por lo tanto, deje de funcionar correctamente. (Kaspersky, n.d.)

Un servidor de control y comando es una computadora que manda órdenes a dispositivos infectados con malware, permitiéndote recibir información de estos. (Electronic Frontier Foundation, n.d.)

Un botmaster es una persona que opera un servidor de control y comando. (Radware, n.d.)

Sí, la computadora de Jennifer fue infectada por malware el 17 de agosto, cuando se conectó al sitio anómalo por medio del puerto 443.

Ese mismo día, la computadora de Jennifer se conectó a 287 computadoras en la red interna, lo que podría indicar que se realizó un ping sweep.

A partir de entonces puede observarse que la misma computadora realizaba solicitudes diarias a la dirección anómala. Esto puede indicar que se realizó un ataque DDoS.

Por lo tanto, puede identificarse que un botmaster usaba un servidor de control y comando para mandar las instrucciones a las computadoras infectadas.

Reflexiones

Emiliano:

El uso de grafos para la visualización de conexiones en redes es útil dada su cercanía al comportamiento real y su similitud. La adyacencia de nodos permite ingresar las conexiones direccionadas, de manera que se sepa cuál fue el sistema que recibió la conexión, al igual que la cantidad de veces que esto sucedió al ingresar este valor a la adyacencia, la arista.

La implementación es un poco compleja por lo abstractos que pueden ser, y si se hace de manera incorrecta puede no haber conexiones discernibles o errores importantes en estas. Si se hace de la manera apropiada, en cambio, la naturaleza de la estructura para manejar múltiples apuntadores a distintos objetos desde un solo objeto central facilita mucho un análisis de redes. Las aristas permiten visualizar conexiones potencialmente inseguras o extrañas cuando se les agrega un valor significativo, claro que debe simbolizar una característica de la conexión pertinente.

Do Hyun:

Los grafos son estructuras de datos que utilizamos en la vida cotidiana. Facebook, Google, Uber, Quora, todos utilizan grafos. Mediante el uso de gráficos se puede crear cualquier sitio de red social. Las personas representan a los vértices, mientras que la conexión entre ellos es la arista. Los grafos son fáciles de implementar mediante el uso de la lista o matriz y disponemos de esta flexibilidad para elegir la representación de acuerdo a sus necesidades.

Nos permiten almacenar información sobre la relación entre los diferentes componentes (también conocidos como nodos). Estos componentes pueden ser un conjunto de amigos, edificios, calles o cualquier cosa que pueda estar conectada a otra cosa. En el caso

de la presente situación problema, serían las computadoras. Estas computadoras serán los vértices y las conexiones que tienen con otras computadoras se verán representadas como las aristas.

Los grafos te permiten almacenar esta información de forma que te facilita la creación/implementación de los diferentes algoritmos para resolver problemas, desde comprobar si los nodos están conectados hasta encontrar los caminos más cortos.

Referencias:

Electronic Frontier Foundation. (n.d.). *Servidor de Control y Comando*. SURVEILLANCE SELF-DEFENSE. https://ssd.eff.org/es/glossary/servidor-de-control-y-comando

Kaspersky. (n.d.). *¿Qué son los ataques DDoS?* Kaspersky Latinoamérica. https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Ping Sweep. (n.d.). Glosario Terminología Informática. http://www.tugurium.com/gti/termino.php?Tr=ping%20sweep Radware. (n.d.). *Botmaster*. DDoS Attack Definitions - DDoSPedia.

https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/#:~:text=A%20botmaster%20is%20a%20person,forms%20of%20remote%20code%20installation