# Reflexión Actividad 4.2

**Ping sweep**: un ping sweep es una técnica de diagnóstico utilizada en la informática para ver qué rango de direcciones de Protocolo de Internet (IP) utilizan los hosts en vivo. Por lo general se utiliza para indicar dónde están las máquinas activas de una red, y a veces lo utiliza un administrador de sistema para diagnosticar un problema de red.

**DDoS**: son las siglas de Distributed Denial of Service, que se puede interpretar como un ataque al servidor desde muchos ordenadores para que deje de funcionar. Cuando un servidor recibe demasiadas peticiones, comienza a dejar de funcionar, por lo que hasta que el atacante pare, o se bloqueen las conexiones ilegítimas, el servidor seguirá sin funcionar adecuadamente.

**Servidor de comando y control**: es un computador que da ordenes a dispositivos infectados con malware y que recibe información de esos dispositivos. Algunos servidores controlan millones de dispositivos.

**Botmaster**: es una persona que opera el comando y control de una botnet para su ejecución remota. El botmaster usualmente esconderá su identidad por medio de proxies, TOR o shells para disfrazar su dirección IP. En ocasiones una botnet está compartida y puede ser operada por varios botmasters.

El ping sweep en la actividad puede ser lo que hicimos con los grafos para analizar las conexiones anómalas, el DDoS se puede identificar en el pico repentino el día 20 en la página steamcommunity.com, el servidor de comando y control sería el computador que inició el ataque, que pertenecería al botmaster.

**Reflexión importancia de grafos**

Uno de los posibles y mayores beneficios de utilizar grafos para este tipo de problemas es el rápido acceso a la información, dado que no están acomodados de forma parecida a un árbol o lista o sus derivados, pues se puede tomar un vértice y navegar y manipular desde el mismo, sin la necesidad de recorrer los anteriores.

Otro beneficio es que se asemejan al comportamiento real que tienen este tipo de interacciones entre computadoras y servidores, pues los vértices pueden ser: las computadoras, los sitios web, las direcciones IP, etc. Y pueden contener información clave dentro de las mismas o en sus aristas, aparte de poder apoyarse de las demás estructuras de datos, por ejemplo: se puede tener un grafo de conexiones a sitios web, con el número de conexiones contenido en las aristas, y los vértices conteniendo un mapa de una combinación de datos, tales como fecha, direcciones IP, identificadores de la computadora de origen, etc.

**Referencias**

Netinbag (n.d.) *¿Qué es un barrido de ping?*. Recuperado de: https://www.netinbag.com/es/internet/what-is-a-ping-sweep.html

Julián, G. (2016) *¿Qué es un ataque DDoS y cómo pararlo?*. Recuperado de: https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta

Surveillance Self-Defence (n.d.) *Servidor de Control y Comando*. Recuperado de: https://ssd.eff.org/es/glossary/servidor-de-control-y-comando

Radware (n.d.) *Botmaster*. Recuperado de: https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/

Dawson, D. (2020) *Identifying malicios IoT botnet activity using graph theory*. Recuperado de: https://blog.apnic.net/2020/07/16/identifying-malicious-iot-botnet-activity-using-graph-theory/