Tecnológico de Monterrey

Campus Santa Fe (CSF)

Programación de Estructura de Datos y Algoritmos

Actividad 2.2: Actividad Integral de Estructura de Datos Lineales

Integrantes:

García Puebla Diego Fernando - A01028597

Serrano Diego Andrea - A01028728

Fecha de entrega: 21 de Noviembre de 2021

Profesor: Nonell Cubells Vicente

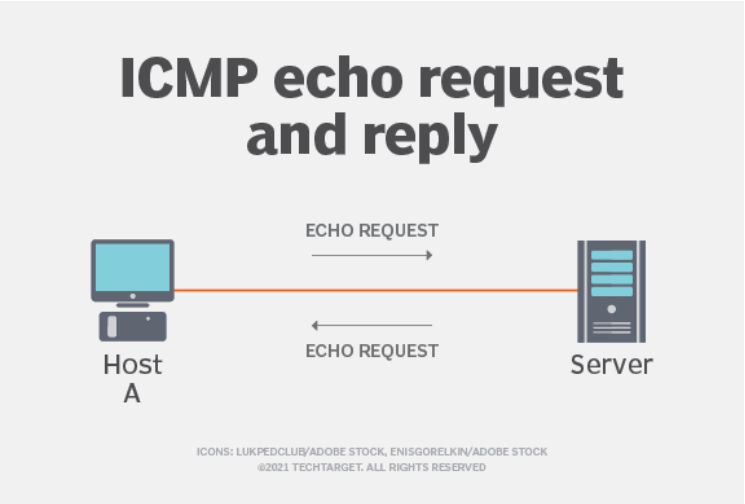
Equipo: 7

Investigación

Ping Sweep

Un ping sweep (conocido en español como un barrido de ping) básicamente es una técnica de escaneo de red que se implementa con el fin de determinar cuál rango de direcciones IP se asigna a hosts activos (que vienen siendo computadoras).

Un barrido de ping consiste en solicitudes de eco *ICMP* (Protocolo de mensajes de control de Internet) enviadas a múltiples hosts (generalmente computadoras). Para poder llevar a cabo esta acción, el ping requiere una dirección a la que enviará la solicitud de eco, que puede ser una dirección IP o un nombre de dominio de servidor web.



La importancia de los barridos de ping es demasiada, debido a que además de identificar los dispositivos activos en una red, también son útiles para detectar dispositivos no reconocidos que pueden ser maliciosos y garantizar que los dispositivos funcionen correctamente. *(Terrell, 2021)*

DDoS

Un DDoS (o también conocido como un ataque distribuido de denegación de servicio) es una extensión de un DoS (ataque de denegación de servicio) que se lleva a cabo a partir de la generación de un gran flujo de información o peticiones desde diferentes dispositivos (fuentes) hacia un punto fijo

La diferencia entre ambos conceptos se da en el hecho de que un ataque DoS tiene una única fuente de origen, mientras que en un ataque DDoS proviene de diferentes fuentes de origen. Por eso mismo el nivel de dificultad de un ataque DDoS es mucho mayor.

Ambos ataques consisten en el envío masivo y simultáneo de determinados paquetes de datos a un objetivo específico, por lo general un servidor web, afectando su capacidad de procesamiento al verse superado, por lo tanto, este colapsa. Como consecuencia de esto, los servicios interrumpen sus operaciones normales y los usuarios legítimos no pueden acceder a los sitios. *(Welivesecurity, 2021)*

Servidor de comando y control

Un servidor de comando y control (servidor C&C o C2) es un método de ataque especialmente insidioso y astuto, debido a que solo una computadora infectada puede destruir una red completa. Una vez que el malware se ejecuta en una máquina, el servidor de C&C puede ordenarle que se duplique y se propague, lo que puede suceder fácilmente, porque ya pasó el firewall de la red.

Una vez que la red está infectada, el atacante puede apagarla o cifrar los dispositivos infectados para bloquear a los usuarios. Por ejemplo, los famosos ataques de *ransomware WannaCry* en 2017 hicieron exactamente eso al infectar computadoras en instituciones críticas como hospitales, bloquearlas y exigir un rescate en bitcoin. (BeeBright, 2021)

Botmaster

La palabra botmaster surge de la unión de dos palabras, en este caso es ‘bot’ que es una aféresis de robot y ‘master’ palabra de la lengua inglés que significa maestro. Y esta palabra se le asigna a las personas encargadas de administrar, crear, programar, y mantener un chatbot. *(L, 2019)*

Pero, ¿Qué es un chatbot?, pues es un programa de inteligencia artificial (IA) que puede simular una conversación (o un chat) con un usuario en lenguaje natural a

través de aplicaciones de mensajería, sitios web, aplicaciones móviles o por teléfono.

Por ejemplo. Si desea comprar zapatos en su tienda minorista local, debe acceder a su sitio web, encontrar lo que está buscando y comprarlo. Pero, ¿y si esa tienda tuviera un bot? Solo sería necesario escribir un mensaje a la marca a través de Facebook y decirles lo que queremos. Y si tenía dudas sobre las medidas de tamaño, podría obtener respuestas a su problema en un momento (e incluso de inmediato). *(Boris, 2020)*

¿Identificas estos elementos en tus datos?

Sí, en esta situación problema (hasta lo que hemos podido realizar), podemos llegar a identificar ciertos elementos como lo son el hecho de que en los datos del archivo "equipo7.csv" se puede llegar a observar un método de ataque como el de servidor de comando y control. Debido a que se puede llegar a observar que hay demasiadas repeticiones de sitios raros, y eso puede llegar a dañar nuestra computadora y generar problemas a nivel de software. Igualmente, se pueden llegar a identificar términos como la de Botnet (y por lo mismo Botmaster), ya que tenemos demasiados datos (de diferentes redes), por lo tanto, se convierte en una botnet.

De igual manera un concepto como el ping sweep, lo podemos llegar a implementar e identificar en nuestros datos (de la situación problema), debido a que este, nos va a ayudar a poder identificar dispositivos no reconocidos que pueden llegar a ser dañinos, además de garantizar que los dispositivos no dañinos funcionen correctamente. Finalmente, se puede decir que estos conceptos se relacionan entre sí y que directamente e indirectamente tienen una gran repercusión en nuestros dispositivos, debido a que pueden afectar (de manera buena o no) nuestro software (e incluso el hardware).

Reflexión Final

La principal importancia de los grafos es la flexibilidad al usarlos en comparación a los árboles binarios, haciendo la creación de mapas más eficiente. Para este problema son necesarios para saber como se conecta cada computadora y poder analizar la información para en este caso descubrir el bootmaster.

Listado de referencias

BeeBright. (2021, 25 junio). *¿Qué es un «servidor de comando y control» para malware?* ResponTodo. Recuperado 19 de noviembre de 2021, de https://respontodo.com/que-es-un-servidor-de-comando-y-control-para-malware/

Boris, B. (2020, 21 octubre). *¿Qué es un Chatbot y para que sirve?* Efectovisual. Recuperado 19 de noviembre de 2021, de https://www.efectovisual.cl/blog/85-que-es-un-chatbot-y-para-que-sirve.html

L. (2019, 3 julio). *¿Qué es un botmaster?* Botifica. Recuperado 19 de noviembre de 2021, de https://botifica.com/blog/que-es-un-botmaster/

Terrell, K. (2021, 18 junio). *ping sweep (ICMP sweep)*. SearchNetworking. Recuperado 19 de noviembre de 2021, de https://www.techtarget.com/searchnetworking/definition/ping-sweep-ICMP-sweep

Welivesecurity. (2021, 2 septiembre). *Qué es un ataque DDoS y cuáles son sus consecuencias*. Welivesecurity.com. Recuperado 19 de noviembre de 2021, de https://www.welivesecurity.com/la-es/2021/09/02/que-es-ataque-ddos/