Diego Mejía - A01024228
Enrique Mondelli - A01379363

Reporte Reto 5

A: 192.168.155.57
B: x6s57cx25hchyzsyv9oh.com
C: live.com

1. **¿Es A el vértice que más conexiones salientes hacia la red interna tiene?**
2. **¿Existen conexiones de las demás computadoras hacia A?**

Se muestra la fecha de los grafos, y las respuestas por día de las preguntas 1 y 2.

10-8-2020:
1. No
2. No

11-8-2020:
1. No
2. No

12-8-2020:
1. No
2. No

13-8-2020:
1. No
2. No

14-8-2020:
1. No
2. No

17-8-2020:
1. Sí
2. Sí

18-8-2020:
1. No
2. Sí

19-8-2020:
1. Sí
2. Sí

20-8-2020:
1. No
2. Sí

21-8-2020:

1. No
2. Sí

3. **Determina cuántas computadoras se han conectado a B por día**
4. **Indica cuántas computadoras se han conectado a C por día.**

Se muestra la fecha de los grafos, y las respuestas por día de las preguntas 3 y 4.

10-8-2020:
3. 0
4. 7

11-8-2020:
3. 0
4. 6

12-8-2020:
3. 0
4. 10

13-8-2020:
3. 0
4. 8

14-8-2020:
3. 0
4. 13

17-8-2020:
3. 1
4. 7

18-8-2020:
3. 1
4. 9

19-8-2020:
3. 1
4. 32

20-8-2020:
3. 1
4. 7

21-8-2020:
3. 1
4. 10

A continuación, se presentarán los términos de pings sweep, DDoS, servidor de comando y control, y botmaster.

ping sweep: “Ataque que envía peticiones de eco ICMP, "pings", a un rango de direcciones IP, con el objetivo de encontrar anfitriones que se pueden probar en busca de vulnerabilidades” (Glosario Terminología Informática, 2016).

DDoS: “Denegación de Servicio Distribuido” (Glosario Terminología Informática, 2000).

servidor de comando y control: “Un Servidor de Control y Comando (C&C o C2) es un computador que da órdenes a dispositivos infectados con malware y que recibe información de esos dispositivos” (Surveillance Self-Defense, s.f).

botmaster: “El Botmaster es el responsable de enseñar, gestionar y mantener el chatbot.” (Prada, J., 2019).

De acuerdo a lo anterior, y después de haber hecho un análisis de los datos proveídos para la realización de este reto, se puede observar una caso de ping sweep. De acuerdo a los resultados obtenidos, solo existe una ip de la red interna que se está conectando al sitio web sospechoso, lo cual puede ser inferido a que esta computadora ha sido infectada debido a que se encontró una vulnerabilidad en el sistema.

Todo esto posiblemente causado por un ataque DDoS que puede que esté denegando acceso al usuario legítimo de la computadora, haciendo uso de dicha ip de manera maliciosa, y en este caso, para conectarse al dominio con nombre sospechoso.

En adición a esto la razón por la que esto sucede es por un servidor de comando y control que está enviando instrucciones al ordenador infectado, todo esto siendo controlado por un posible botmaster, que obtuvo acceso a la red interna gracias a este ataque y las instrucciones que da para que se conecte a la página sospechosa.

Aportaciones Individuales

Enrique:
Yo contribuí con la realización de la programación del archivo principal, “main.cpp”, al hacer la lógica para crear los grafos por dia con sus filtros adecuados, ya sea de conexiones internas o conexiones a sitios web, y la lógica para responder las preguntas del reto con la información adquirida al crear dichos grafos.

Diego:
Durante la realización del quinto reto, yo realice la organización y escritura del reporte con las preguntas, así cómo la investigación de los conceptos requeridos de acuerdo a las instrucciones, además de su relación con los datos obtenidos.

Referencias

Glosario Terminología Informática. (2016). *ping sweep* [Página Web]. Recuperado de: http://www.tugurium.com/gti/termino.php?Tr=ping%20sweep
Glosario Terminología Informática. (2000). *ddos* [Página Web]. Recuperado de: http://www.tugurium.com/gti/termino.php?Tr=ddos
Surveillance Self-Defense. (s.f.). *Servidor de Control y Comando* [Página Web]. Recuperado de: https://ssd.eff.org/es/glossary/servidor-de-control-y-comando#:~:text=Un%20Servidor%20de%20Control%20y,servidores%20controlan%20millones%20de%20dispositivos
Prada, J. (2019). *BOTMASTER, ¿El empleo del futuro?* [Página Web]. Recuperado de: https://cepymenews.es/botmaster-empleo-futuro/#:~:text=El%20Botmaster%20es%20el%20responsable,a%20un%20tema%20en%20concreto.