DESAFÍO 1 - RASTREO DE ATAQUE PCAP - (PROPORCIONADO POR TILLMANN WERNER) CONSISTE EN INVESTIGAR UN ATAQUE DE RED.

EL DESAFÍO:

Se proporciona un rastreo de red con datos de ataque. (Tenga en cuenta que la dirección IP de la víctima se ha cambiado para ocultar la verdadera ubicación). Analice y responda a las siguientes preguntas:

1. ¿Qué sistemas (es decir, direcciones IP) están implicados? (2pts)
2. ¿Qué puede averiguar sobre el host atacante (por ejemplo, dónde está ubicado)? (2pts)
3. ¿Cuántas sesiones TCP contiene el archivo de volcado? (2pts)
4. ¿Cuánto tiempo se tardó en realizar el ataque? (2pts)
5. ¿A qué sistema operativo iba dirigido el ataque? ¿Y a qué servicio? ¿Qué vulnerabilidad? (6pts)
6. ¿Puede esbozar un resumen de las acciones generales realizadas por el atacante? (6pts)
7. ¿Qué vulnerabilidad específica fue atacada? (2pts)
8. ¿Qué acciones realiza el shellcode? Por favor, enumere el shellcode. (8pts)
9. ¿Cree que se utilizó un Honeypot para hacerse pasar por una víctima vulnerable? ¿Por qué? (6pts)
10. ¿Hubo malware involucrado? ¿Cuál es el nombre del malware? (No estamos buscando un análisis detallado del malware para este desafío) (2pts)
11. ¿Cree que se trata de un ataque manual o automatizado? ¿Por qué? (2pts)