Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
El protocolo **UDP** revela que el navegador envió solicitudes DNS al servidor **203.0.113.2** para obtener la dirección IP del dominio **www.yummyrecipesforme.com**. Estas solicitudes se enviaron específicamente al **puerto 53**, que es el puerto estándar utilizado por el servicio DNS. Según los resultados del análisis de red, las respuestas ICMP muestran repetidamente el mensaje de error: **“puerto udp 53 inalcanzable”** Este mensaje indica que el servidor DNS no pudo entregar la respuesta porque **no había ningún servicio escuchando en el puerto 53**, o el puerto estaba bloqueado o inaccesible. El puerto mencionado en el mensaje de error, **UDP 53**, se utiliza para: ● **Consultas DNS**, que permiten traducir nombres de dominio en direcciones IP. El problema más probable es: ● **El servidor DNS no está respondiendo en el puerto 53**, ya sea por una falla del servicio, una mala configuración, o un bloqueo en la red que impide que las solicitudes DNS lleguen correctamente. ● Como consecuencia, el navegador no puede obtener la dirección IP del sitio web y no puede cargar la página.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Hora en que ocurrió el incidente:

El registro tcpdump muestra marcas de tiempo como **13:24:32.192571**, lo que indica que el incidente ocurrió alrededor de las **13:24 horas**.

Cómo el equipo de TI se dio cuenta del incidente:

Varios clientes reportaron que no podían acceder al sitio web **www.yummyrecipesforme.com** y recibían el mensaje **"puerto de destino inalcanzable"**. El analista también intentó acceder al sitio y obtuvo el mismo error.

Acciones tomadas por el departamento de TI:

- Se intentó cargar la página web desde un navegador.
- Se ejecutó **tcpdump** para capturar el tráfico de red.
- Se analizaron las solicitudes DNS enviadas por UDP y las respuestas ICMP recibidas.
- Se identificó que el servidor DNS devolvía errores de puerto inalcanzable.

Hallazgos clave de la investigación:

- El navegador envió solicitudes DNS por **UDP al puerto 53** del servidor **203.0.113.2**.
- El servidor DNS respondió con mensajes **ICMP "puerto udp 53 inalcanzable"**.
- Esto indica que el servicio DNS no estaba disponible o no estaba escuchando en el puerto 53.
- Sin una respuesta DNS válida, el navegador no puede obtener la dirección IP del sitio web y no puede iniciar la conexión HTTPS.

Causa probable del incidente:
La causa más probable es que **el servicio DNS del servidor 203.0.113.2 está caído, mal configurado o bloqueado**, lo que impide que responda a las solicitudes DNS en el puerto 53.

Esto provoca que los clientes no puedan resolver el dominio y, por lo tanto, no puedan acceder al sitio web.