Security incident report

Sección 1: Identificar el protocolo de red involucrado en el incidente
El protocolo UDP revela que: 53 TCP/UDP Sistema de nombres de dominio (DNS) Esto se basa en los resultados del análisis de la red, que muestran que la respuesta de eco ICMP 203.0.113.2 es el inicio del mensaje de error que indica que el paquete UDP no se pudo entregar en el puerto 53 del servidor DNS. devolvió el mensaje de error:"puerto udp 53 inalcanzable" El puerto indicado en el mensaje de error se utiliza para:La palabra "inalcanzable" en el mensaje indica que el mensaje UDP que solicitaba una dirección IP para el dominio en cuestión no llegó al servidor DNS porque no había ningún servicio escuchando en el puerto DNS receptor. El problema más probable es:esto puede ser a sobrecarga del puerto o una denegación de servicio por parte de un agente externo, es posible que esto sea un indicio de un ataque malicioso al servidor web.

Sección 2: Documentar el incidente
Hora en que ocurrió el incidente: 13:24:32,192571. Explique cómo el equipo de TI se enteró del incidente:Varios clientes informaron que durante esa mañana no pudieron acceder al dominio y les daba un error al no encontrar respuesta luego de una espera, esperando que cargaran los datos de la web. Explique las acciones tomadas por el departamento de TI para investigar el incidente: en primer lugar se llama a los analistas para investigar el error ocurrido a los usuarios .Se recrean las condiciones y con la ayuda el registro tcpdump se establece que pasa al resolver el DNS solicitado.Luego de determinar el incidente se pasa al siguiente grupo Tenga en cuenta los hallazgos clave de la investigación del departamento de TI (es decir, detalles relacionados con el puerto afectado, servidor DNS, etc.): el puerto afectado fue el 53 el que resuelve los

dns (de nombres pasa a ip para lograr comunicarse con el servicio o web solicitados).se determinó que al pedir resolverlo el puerto no respondía, no tenía un servicio asociado.
Tenga en cuenta una causa probable del incidente: se investiga pero dados los resultados puede ser denegación de servicio(DOS) que busca sobrecargar a peticiones un servicio hasta que este se ve abrumado y termina por caer y dejar de ofrecer servicio.

Sección 3: Recomendar una solución para ataques de fuerza bruta
Primero sería investigar a fondo el asunto para determinar cuál vía utilizaron para lograr denegar el servicio. Luego mejorar las condiciones de seguridad (reducir superficie de ataque, mejorar claves y revisar los protocolos de red) y hacer pruebas buscando alguna otra vulnerabilidad. Y si fue denegación de servicio o a fuerza bruta determinaron credenciales con las cuales desactivan el sistema.