El ejemplo explicado   
Informe sobre incidentes de ciberseguridad: análisis del tráfico de red

| Parte 1: Proporcione un resumen del problema encontrado en el registro de tráfico DNS e ICMP | | Explicación |
| --- | --- | --- |
| 1. El protocolo UDP revela que el servidor DNS está inactivo o no se puede acceder a él. 2. Como lo evidencian los resultados del escaneo de red, la respuesta de eco ICMP devolvió el mensaje de error: "puerto udp 53 inalcanzable". 3. El puerto 53 se utiliza habitualmente para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no esté respondiendo. | | 1. **Ofrece un breve resumen del análisis del registro ICMP y DNS.** Siguiendo las instrucciones, debería haber identificado "qué protocolo de red y servicio se vieron afectados por este incidente". El escenario indica: "[El archivo de registro] muestra qué protocolo se utilizó para gestionar las comunicaciones y a qué puerto se enviaron. En el registro de errores, esto se muestra como puerto UDP 53 inaccesible. Esto significa que se utilizó el protocolo UDP para solicitar una resolución de nombre de dominio utilizando la dirección del servidor DNS a través del puerto 53". 2. **Proporciona algunos detalles sobre lo que se indicó en los registros:** la sección Escenario indica que realizó un análisis de red utilizando tcpdump, que registró los paquetes ICMP desde su computadora de origen a la dirección IP y el puerto del sitio web (203.0.113.2.domain). También registró las respuestas ICMP del sitio web a su computadora. Si revisa el registro de errores de DNS e ICMP, las respuestas de ICMP incluyen un tipo de mensaje de error que tcpdump representa como “puerto udp 53 inalcanzable”. 3. **Interprete los problemas que se encuentran en los registros.** La sección Escenario (o una búsqueda rápida en Internet de “puerto 53”) mostrará que este número de puerto se usa comúnmente para las comunicaciones del protocolo DNS.Dado que el puerto 53 no es accesible y ese puerto se usa comúnmente para las comunicaciones del servidor DNS, se puede concluir que el servidor DNS no es accesible o que “no responde”. Esto podría deberse, por ejemplo, a un ataque DoS contra el servidor DNS. |
|

| Parte 2: Explique su análisis de los datos y proporcione una solución para implementar | Explicación |
| --- | --- |
| 1. El incidente ocurrió hoy a las 13:23 horas. 2. Los clientes llamaron a la organización para notificar al equipo de TI que recibieron el mensaje “puerto de destino inalcanzable” cuando intentaron visitar el sitio web. 3. Los profesionales de seguridad de red de la organización están investigando actualmente el problema para que los clientes puedan acceder nuevamente al sitio web. 4. En nuestra investigación del problema, realizamos pruebas de rastreo de paquetes con tcpdump. En el archivo de registro resultante, descubrimos que no se podía acceder al puerto DNS 53. 5. El siguiente paso es identificar si el servidor DNS está inactivo o el tráfico al puerto 53 está bloqueado por el firewall.      1. El servidor DNS podría estar inactivo debido a un ataque de denegación de servicio exitoso o una configuración incorrecta. | 1. **Indica cuándo se informó el problema por primera vez:** Esta información se obtuvo de las marcas de fecha y hora del archivo de registro. En el registro, esta es la primera secuencia de números que se muestra: 13:24:32.192571. Esto muestra la hora 1:24 pm, 32.192571 segundos, con la hora en formato de 24 horas. El escenario indica que este evento ocurrió hoy. 2. **Proporciona el escenario, los eventos y los síntomas identificados cuando se informó el evento por primera vez:** el escenario establece que “Un puñado de clientes se comunicaron con su empresa para informar que no podían acceder al sitio web de la empresa y vieron el error “puerto de destino inalcanzable” después de esperar a que se cargara la página”. 3. **Explica el estado actual del problema:** el escenario establece que "mientras tanto, los ingenieros de seguridad están manejando este incidente después de que usted y otros analistas hayan informado el problema a su supervisor directo". 4. **Describe la información descubierta a partir de la investigación del problema hasta este momento:** proporciona un resumen conciso de lo que hizo para investigar el problema. El escenario indica: "Visita el sitio web y también recibe el error "puerto de destino inalcanzable". A continuación, carga su herramienta de análisis de red, tcpdump, y carga la página web nuevamente. Esta vez, recibe muchos paquetes en su analizador de red. En el analizador, envía paquetes UDP y recibe una respuesta ICMP para regresar al host. Los resultados contienen un mensaje de error: "puerto udp 53 inalcanzable".      1. **Enumera los pasos siguientes para solucionar el problema:** El siguiente paso para solucionar el problema es determinar si el servidor DNS no está funcionando correctamente. Si el servidor DNS está bien, el equipo debe verificar la configuración del firewall para ver si alguien cambió la configuración para bloquear el tráfico de red en el puerto 53. Los firewalls ofrecen la capacidad de bloquear el tráfico de red en puertos específicos. El bloqueo de puertos se puede utilizar para detener o prevenir un ataque. 2. **Proporciona la causa raíz sospechada del problema:** Anteriormente, aprendió sobre varios tipos de ataques de denegación de servicio (DoS). El objetivo de un ataque DoS es enviar una avalancha de información a un dispositivo de red, como un servidor DNS, para bloquearlo o impedirle responder al tráfico legítimo de la red. Es posible que un atacante haya desactivado el servidor DNS con un ataque DoS. Alternativamente, alguien de su equipo podría haber realizado un cambio de configuración en el firewall que bloqueó el puerto 53. |