Cybersecurity Incident Report: Analysis de trafico de red

Parte 1: Proporcione un resumen del problema detectado en el registro de tráfico DNS e ICMP.	Explicación
A. Como parte del protocolo DNS, se utilizó el protocolo UDP para contactar con el servidor DNS y recuperar la dirección IP del nombre de dominio yummyrecipesforme.com. Se utilizó el protocolo ICMP para responder con un mensaje de error, indicando problemas al contactar con el servidor DNS. B. El mensaje UDP que va desde su navegador al servidor DNS se muestra en las dos primeras líneas de cada evento de registro. La respuesta de error ICMP del servidor DNS a su navegador se muestra en la tercera y cuarta línea de cada evento de registro con el mensaje de error «udp port 53 unreachable» (puerto udp 53 inaccesible). Dado que el puerto 53 está asociado al tráfico del protocolo DNS, sabemos que se trata de un problema	A. **Incluya un breve resumen del análisis del registro de tcpdump e identifique qué protocolos se utilizaron para el tráfico de red.** el escenario resume el problema e identifica los protocolos utilizados. El escenario dice lo siguiente: «Para cargar la página web, el navegador envía primero una consulta a un servidor DNS a través del protocolo UDP para recuperar la dirección IP del nombre de dominio del sitio web; esto forma parte del protocolo DNS... El analizador muestra que, cuando se envían paquetes UDP al servidor DNS, se reciben paquetes ICMP que contienen el mensaje de error: «udp port 53 unreachable» (puerto UDP 53 inaccesible). B. **Proporcione algunos detalles sobre lo que se indicaba en el registro.** El primer y segundo paso de la sección del escenario indican que realizó un análisis de red utilizando tcpdump, que registró los paquetes UDP desde su ordenador de origen a la dirección IP y el puerto del servidor DNS (203.0.113.2.dominio). También registró las respuestas de error ICMP del servidor DNS a su ordenador con el mensaje de error «udp port 53 unreachable» (puerto udp 53 inaccesible). En el sexto paso mencionamos que «el puerto 53 es un puerto para el servicio DNS», lo que significa que se trata de un problema con el servidor DNS. Incluimos más indicios de problemas con el rendimiento del DNS en el quinto paso del escenario: «El signo más después del número de identificación de la consulta indica que hay

con el servidor DNS. Los problemas con la ejecución del protocolo DNS son aún más evidentes porque el signo más después del número de identificación de la consulta 35084 indica indicadores con el mensaje UDP y el símbolo «A?» indica indicadores con la ejecución de operaciones del protocolo DNS. C. Debido al mensaje de respuesta de error ICMP sobre el puerto 53, es muy probable que el servidor DNS no esté respondiendo. Esta suposición se ve respaldada por los indicadores asociados con el mensaje UDP saliente y la recuperación del nombre de dominio.	indicadores asociados al mensaje UDP. La «A?» indica un indicador asociado a la solicitud DNS de un registro A, donde un registro A asigna un nombre de dominio a una dirección IP». C. Interprete los problemas encontrados en el registro. La sección Escenario (o una búsqueda rápida en Internet de «puerto 53») mostrará que este número de puerto se utiliza habitualmente para las comunicaciones del protocolo DNS. Dado que no se puede acceder al puerto 53 y que dicho puerto se utiliza habitualmente para las comunicaciones del servidor DNS, se puede concluir que no se puede acceder al servidor DNS 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 al menos una causa del incidente.	Explanation

D. El incidente ocurrió hoy a la 1:24 p. m. Los clientes notificaron a la organización que recibieron el mensaje «puerto de destino inaccesible» cuando intentaron visitar el sitio web yummyrecipesforme.com. E. El equipo de ciberseguridad que presta servicios de TI a la organización de sus clientes está investigando el problema para que los clientes puedan volver a acceder al sitio web. F. En nuestra investigación sobre el tema, realizamos pruebas de sniffing de paquetes utilizando tcpdump. En el archivo de registro resultante, descubrimos que no se podía acceder al puerto 53 del DNS. G. H.	D. **Indique cuándo se informó del 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 p. m., 32.192571 segundos, con la hora en formato de 24 horas. El escenario indica que este evento ocurrió hoy. E. **Proporcione el escenario, los eventos y los síntomas identificados cuando se informó por primera vez del evento.** The Scenario states that, “A handful of customers contacted your company to report that they were not able to access the company website, and saw the error “destination port unreachable” after waiting for the page to load.” F. **Explica el estado actual del problema** El escenario establece que «Mientras tanto, este incidente está siendo gestionado por ingenieros de seguridad después de que usted y otros analistas hayan informado del problema a su supervisor directo». G. **Describa la información descubierta al investigar el problema hasta el momento.** Proporciona un resumen conciso de lo que hiciste para investigar el problema. El escenario dice: «Visitas el sitio web y también recibes el error «puerto de destino inaccesible»». A continuación, carga su herramienta de análisis de red, tcpdump, y vuelve a cargar la página web. Esta vez, recibe muchos paquetes en su analizador de red. En el analizador, envía paquetes UDP y recibe una respuesta ICMP para volver al host. Los resultados contienen un mensaje de error: «puerto udp 53 inaccesible». H. **Enumere los siguientes pasos para solucionar el problema y resolverlo.**

El siguiente paso es identificar si el servidor DNS está caído o si el tráfico al puerto 53 está bloqueado por el firewall. I. El servidor DNS podría estar inactivo debido a un ataque de denegación de servicio exitoso o a una configuración incorrecta.	El siguiente paso en la resolución de problemas es determinar si el servidor DNS no funciona correctamente. Si el servidor DNS funciona correctamente, el equipo debe comprobar la configuración del cortafuegos para ver si alguien ha cambiado la configuración para bloquear el tráfico de red en el puerto 53. Los cortafuegos ofrecen la posibilidad de bloquear el tráfico de red en puertos específicos. El bloqueo de puertos se puede utilizar para detener o prevenir un ataque. I. **Indique la causa principal sospechada del problema.** Anteriormente, aprendiste 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 impedir que responda al tráfico de red legítimo. Es posible que un atacante haya desactivado el servidor DNS con un ataque DoS. Alternativamente, alguien de tu equipo podría haber realizado un cambio de configuración en el firewall que bloqueó el puerto 53.