Contexto

Varios clientes se pusieron en contacto con tu empresa para informar que no podían acceder al sitio web de la empresa www.yummyrecipesforme.com, y vieron el error “puerto de destino inalcanzable” después de esperar a que se cargara la página.

Tienes la tarea de analizar la situación y determinar qué protocolo de red se vio afectado durante este incidente. Para empezar, visitas el sitio web y también recibes el error “puerto de destino inalcanzable”. A continuación, cargas tu herramienta de análisis de red, tcpdump, y vuelves a cargar la página web. Esta vez, recibes una gran cantidad de paquetes en tu analizador de red. El analizador muestra que cuando envías paquetes UDP y recibes una respuesta ICMP devuelta a su host, los resultados contienen un mensaje de error: “udp port 53 unreachable.” (puerto udp 53 inalcanzable).

En el registro DNS e ICMP, encuentras la siguiente información:

1. En las dos primeras líneas del archivo de registro, ves la solicitud inicial saliente de tu computadora al servidor DNS solicitando la dirección IP de yummyrecipesforme.com. Esta solicitud se envía en un paquete UDP.

2. A continuación, encontrarás marcas de tiempo que indican cuándo ocurrió el evento. En el registro, esta es la primera secuencia de números que se muestra. Por ejemplo: 13:24:32.192571. Esto muestra el tiempo 1:24 p. m., 32.192571 segundos.

3. La siguiente es la dirección IP de origen y destino. En el registro de errores, esta información se muestra como: 192.51.100.15.52444 > 203.0.113.2.domain. La dirección IP a la izquierda del símbolo mayor que (>) es la dirección de origen. En este ejemplo, la fuente es la dirección IP de tu computadora. La dirección IP a la derecha del símbolo mayor que (>) es la dirección IP de destino. En este caso, es la dirección IP del servidor DNS: 203.0.113.2.domain

4. La segunda y tercera líneas del registro muestran la respuesta a tu paquete inicial de solicitud ICMP. En este caso, la línea ICMP 203.0.113.2 es el comienzo del mensaje de error que indica que el paquete ICMP no se pudo entregar en el puerto del servidor DNS.

5. A continuación, están el protocolo y el número de puerto, que muestra qué protocolo se utilizó para gestionar las comunicaciones y a qué puerto se entregó. En el registro de errores, esto aparece como “udp port 53 unreachable” (puerto udp 53 inalcanzable). Esto significa que el protocolo UDP se utilizó para solicitar una resolución de nombre de dominio utilizando la dirección del servidor DNS a través del puerto 53. El puerto 53, que se alinea con la extensión .domain en 203.0.113.2.domain, es un puerto bien conocido para el servicio DNS. La palabra “inalcanzable” en el mensaje indica que el mensaje no llegó al servidor DNS. Tu navegador no pudo obtener la dirección IP de yummyrecipesforme.com, que necesita para acceder al sitio web porque ningún servicio estaba escuchando en el puerto DNS receptor, como indica el mensaje de error ICMP “udp port 53 unreachable.” (puerto udp 53 inalcanzable).

6. Las líneas restantes del registro indican que los paquetes ICMP se enviaron dos veces más, pero se recibió el mismo error de entrega en ambas ocasiones.

Ahora que capturaste paquetes de datos utilizando una herramienta de análisis de red, tu trabajo consiste en identificar qué protocolo y servicio de red se vieron afectados por este incidente. Luego, tendrás que redactar un informe de seguimiento.

Como analista, puedes inspeccionar el tráfico de red y los datos de red para determinar qué está causando los problemas relacionados con la red durante los incidentes de ciberseguridad. Más adelante en este curso, demostrarás cómo gestionar y resolver incidentes. Por ahora, solo necesitas analizar la situación. Mientras tanto, este incidente está siendo gestionado por ingenieros de seguridad después de que tú y otros analistas hayan informado del problema a tu supervisor directo.