Informe incidente de ciberseguridad

Escenario

Analiza el siguiente caso. Luego, completa las instrucciones paso a paso.
Eres un analista de ciberseguridad que trabaja en una empresa que se especializa en la prestación de servicios de consultoría informática. 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.

Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP

La herramienta de análisis de tráfico de red inspecciona todos los paquetes IP que viajan a través de las interfaces de red del equipo en el que se ejecuta. Los paquetes de red se registran en un archivo. Tras analizar los datos que se te presentan del registro de tráfico DNS e ICMP, identifica las tendencias en los datos.

Evalúa qué protocolo está produciendo el mensaje de error al resolver la URL con el servidor DNS para el sitio web yummyrecipesforme.com. Recuerda que uno de los puertos que se muestra repetidamente es el puerto 53, comúnmente utilizado para DNS. En tu análisis:

- Incluye un breve resumen del análisis de los registros DNS e ICMP e identifica qué protocolo se utilizó para el tráfico ICMP.
- Proporciona algunos detalles sobre lo que se indica en los registros.
- Interpreta los problemas encontrados en los registros.

Registra tus respuestas en la primera parte del informe sobre incidentes de ciberseguridad.

Resumen del problema encontrado en el registro de tráfico DNS e ICMP
El análisis de la red muestra que se utilizó el **protocolo UDP** para enviar solicitudes al servidor DNS, pero la respuesta indica un problema con el **servidor DNS**. El mensaje de error recibido fue **"udp port 53 unreachable"** (puerto UDP 53 inalcanzable), lo que significa que el servidor DNS no pudo procesar la solicitud en el puerto 53, que es el puerto estándar para los servicios DNS. El análisis de red revela que la respuesta **ICMP** indica que el servidor no pudo ser alcanzado en dicho puerto, lo que impidió al navegador obtener la dirección IP del sitio **yummyrecipesforme.com**.

Explica tu análisis de los datos y proporciona una solución para implementar

Ahora que inspeccionaste el registro de tráfico e identificaste tendencias en el tráfico, describe por qué aparecieron los mensajes de error en el registro. Utiliza tu respuesta del paso anterior y el escenario para identificar el motivo de los mensajes de error ICMP. Los mensajes de error indican que hay un problema con un puerto específico. ¿Qué revelan sobre el incidente los distintos protocolos que aparecen en el registro? En tu respuesta:

- Indica cuándo se notificó el problema por primera vez.
- Proporciona el escenario, los eventos y los síntomas identificados cuando se informó del incidente por primera vez.

- Describe la información descubierta durante la investigación del problema hasta ese momento.
- Explica el estado actual del problema.
- Indica la presunta causa raíz del problema.
- Enumera los siguientes pasos necesarios para solucionar el problema.

Registra tus respuestas en la segunda parte del informe sobre incidentes de ciberseguridad.

Análisis de los datos y posible causa del incidente
Hora del incidente: El incidente ocurrió a las **13:24:32**, cuando se envió la solicitud inicial al servidor DNS y se devolvió el mensaje de error ICMP. **Cómo se detectó el incidente:** El equipo de TI fue informado después de que varios clientes y empleados reportaran la imposibilidad de acceder al sitio web y recibieran el mensaje **"puerto de destino inalcanzable"**. **Acciones tomadas por el equipo de TI:** El equipo de TI utilizó la herramienta de análisis de red **tcpdump** para capturar los paquetes y analizar los errores. Se verificó que el puerto 53, usado para la resolución de nombres de dominio, estaba inalcanzable. **Hallazgos clave:** El servidor DNS responsable de resolver **yummyrecipesforme.com** no estaba disponible para recibir solicitudes en el puerto UDP 53, como lo demuestra el mensaje **"udp port 53 unreachable"**. **Posible causa del incidente:** La causa más probable es que el **servidor DNS** no estaba en funcionamiento o su puerto 53 estaba bloqueado, lo que impidió la resolución del nombre de dominio. Esto pudo deberse a problemas en la configuración del servidor, fallos de red o políticas de firewall mal configuradas que impiden la comunicación en dicho puerto.