Informe de incidente de ciberseguridad:

Análisis de tráfico de red

Ejemplo de incidente

Usted es un analista de ciberseguridad que trabaja en una empresa especializada en la prestación de servicios informáticos para clientes. Varios clientes informaron de que no podían acceder al sitio web de la empresa cliente www.yummyrecipesforme.com, y vieron el error "puerto de destino inalcanzable" después de esperar a que se cargara la página.

Usted tiene la tarea de analizar la situación y determinar qué protocolo de red se vio afectado durante este incidente.

Para empezar, se intenta visitar la página web y también recibe el error "puerto de destino inalcanzable". Para solucionar el problema, se carga la herramienta de análisis de red, ***tcpdump***, y se intenta cargar de nuevo la página web. El analizador muestra que cuando envía paquetes UDP al servidor DNS, recibe paquetes ICMP que contienen el mensaje de error: "Puerto UDP 53 inalcanzable".

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Parte 1: Resumen del problema encontrado en el registro tcpdump

Breve resumen del análisis del registro tcpdump:

Al realizar un análisis de tráfico con ***tcpdump***, se identificó un problema con la resolución DNS. Las solicitudes enviadas a través del protocolo UDP desde el navegador al servidor DNS (203.0.113.2) para resolver el dominio www.yummyrecipesforme.com no recibieron respuesta válida.

Protocolos utilizados:

- UDP (User Datagram Protocol): Utilizado para enviar la solicitud DNS desde el cliente al servidor.

- ICMP (Internet Control Message Protocol): Proporcionó los mensajes de error de red en respuesta a las solicitudes fallidas.

- DNS (Domain Name System): Servicio afectado, que opera sobre UDP en el puerto 53.

Protocolo	Función	Puerto utilizado
UDP	Transporte de solicitudes DNS	53
ICMP	Mensajes de error y diagnóstico de red	N/A
DNS	Resolución de nombres de dominio	53 (sobre UDP)

Detalles del registro:

- La IP de origen es 192.51.100.15 (el cliente).

- La IP de destino es 203.0.113.2 (servidor DNS).

- El mensaje ICMP de error indica que el puerto UDP 53 es “inalcanzable”.

Interpretación del problema:

El mensaje ICMP “puerto UDP 53 inalcanzable” sugiere que no hay un servicio DNS activo o accesible en el servidor. El tráfico UDP no puede alcanzar el puerto 53, lo que impide la resolución de nombres y genera fallos al cargar páginas web como www.yummyrecipesforme.com.

Parte 2: Análisis del incidente y solución

Escenario del incidente:

Varios clientes informaron que no podían acceder al sitio web www.yummyrecipesforme.com.

Al intentar acceder, se mostraba el mensaje de error "puerto de destino inalcanzable". Se utilizó ***tcpdump*** para capturar y analizar el tráfico de red durante la carga del sitio.

Línea de tiempo del incidente según el análisis de la marca de tiempo en el registro ***tcpdump***.

Hora	Evento
13:24:32	Inicio de la solicitud DNS desde el cliente
13:24:32	Recepción del primer mensaje ICMP de error
13:24:33	Repetición de la solicitud DNS
13:24:33	Recepción del segundo mensaje ICMP de error
13:24:34	Tercer intento y tercer mensaje ICMP recibido

Estado actual del problema:

El dominio no puede resolverse porque el servidor DNS no está respondiendo correctamente a las solicitudes de resolución. Las consultas DNS enviadas por el navegador no llegan al destino debido a un problema con el puerto 53.

Información descubierta en la investigación:

- Las solicitudes DNS son enviadas correctamente desde el cliente.

- El servidor DNS responde con mensajes ICMP señalando que el puerto UDP 53 está inalcanzable.

- Se realizaron múltiples intentos, todos con el mismo resultado.

Presunta causa raíz del problema:

El servidor DNS no tiene el puerto 53 disponible, posiblemente debido a un fallo en el servicio, una mala configuración de red o reglas de firewall que impiden la conexión.

Siguientes pasos para resolver el problema:

Paso	Acción
1	Verificar que el servidor DNS tenga el servicio activo.
2	Confirmar que el puerto 53 esté abierto y no bloqueado por el firewall
3	Validar la configuración de red del servidor DNS.
4	Utilizar servidor DNS alternativo (p. ej., 8.8.8.8).
5	Reportar el problema al administrador del servidor DNS.

Conclusión

En conclusión, el análisis evidenció que la causa del incidente se relaciona directamente con la inaccesibilidad del puerto DNS (53) del servidor. Se recomienda revisar la disponibilidad del servicio DNS y aplicar los correctivos indicados para restablecer la conectividad

Glosario

Término	Definición
DNS	Sistema de nombres de dominio. Traduce nombres de sitios web a direcciones IP.
UDP	Protocolo de comunicación sin conexión utilizado por servicios como DNS.
ICMP	Protocolo usado para enviar mensajes de error o diagnóstico en redes IP.
tcpdump	Herramienta de análisis de paquetes de red utilizada para capturar y observar tráfico.