Informe de Incidente de Ciberseguridad

Análisis de Tráfico de Red

Parte 1: Resumen del problema detectado en el análisis de tráfico DNS e ICMP

Durante el análisis de tráfico de red con la herramienta tcpdump, se observó que al intentar resolver el nombre de dominio del sitio web www.yummyrecipesforme.com, el navegador del usuario envía una solicitud DNS utilizando el protocolo UDP al servidor 203.0.113.2 por el puerto 53, que es el puerto estándar del servicio DNS.

La respuesta recibida por parte del servidor fue un mensaje de error ICMP con el contenido:

udp port 53 unreachable

Este mensaje indica que el puerto 53 en el servidor DNS no estaba disponible o no había ningún servicio escuchando en ese puerto en el momento de la solicitud.

Conclusión preliminar:
El servicio DNS, esencial para la resolución de nombres de dominio, no respondió adecuadamente. Esto puede deberse a una caída del servicio, un bloqueo por firewall o un ataque de denegación de servicio (DDoS).

Análisis del incidente y posible causa

Hora del incidente:

Informe de Incidente de Ciberseguridad

El error fue registrado inicialmente a las 13:24:32, y se repitió en intervalos regulares a las 13:26:32 y 13:28:32.

Cómo se detectó el incidente:

Varios usuarios reportaron que no podían acceder al sitio web www.yummyrecipesforme.com. Al intentar cargar la página, recibían el mensaje: "Destination port unreachable".

Acciones realizadas por el equipo de IT:

- Se ejecutó la herramienta de análisis de tráfico tcpdump para capturar los paquetes de red durante el intento de acceso al sitio.
- Se identificaron las solicitudes DNS enviadas y las respuestas ICMP correspondientes.
- Se documentaron las IP involucradas y los puertos afectados.

Hallazgos clave:

- Dirección IP del cliente: 192.51.100.15
- Dirección IP del servidor DNS: 203.0.113.2
- Protocolo utilizado: DNS sobre UDP
- Puerto afectado: 53/UDP
- Mensaje de error: udp port 53 unreachable

Causa probable del incidente:

- El servicio DNS podría estar caído o no estar funcionando correctamente.
- Una mala configuración del servidor o del firewall podría estar bloqueando las solicitudes DNS.
- Existe la posibilidad de un ataque DDoS contra el servidor DNS que impide su funcionamiento normal.