Informe de Incidente de Ciberseguridad
2025

PORT FOLIO

CAMILE
CARRASCO SOTO

camile.dcs@gmail.com

Informe de Incidente de Ciberseguridad:

Análisis del Tráfico de Red – yummyrecipesforme.com

Introducción

El presente informe documenta un incidente de ciberseguridad relacionado con la inaccesibilidad del sitio web www.yummyrecipesforme.com. El incidente fue reportado por varios clientes de clientes que encontraron el mensaje de error **"puerto de destino inalcanzable"** al intentar acceder a la página. Como analista de ciberseguridad, se realizó un análisis detallado del tráfico de red usando la herramienta **tcpdump** para identificar los protocolos afectados, posibles causas y medidas correctivas.

Parte 1: Resumen del problema encontrado en los registros de tráfico DNS e ICMP

Parte 1: Resumen del problema encontrado en los registros de tráfico DNS e ICMP
Protocolo implicado: • **UDP (User Datagram Protocol):** Utilizado para las consultas DNS al servidor 203.0.113.2 solicitando la dirección IP del dominio yummyrecipesforme.com. • **ICMP (Internet Control Message Protocol):** Utilizado por el servidor para notificar errores de entrega de paquetes, en este caso indicando que el puerto 53 es inalcanzable. **Análisis del registro tcpdump:** 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

Interpretación:

1. La primera línea muestra la consulta DNS enviada desde el cliente (IP 192.51.100.15) hacia el servidor DNS (IP 203.0.113.2) a través del **puerto UDP 53**.
2. La segunda línea indica la respuesta ICMP de error: el puerto UDP 53 es **inalcanzable**, lo que significa que el servidor no puede recibir paquetes en ese puerto.
3. Las siguientes solicitudes y respuestas replican el mismo patrón, confirmando que **el problema persiste en múltiples intentos**.

Puerto afectado:

- **Puerto 53 (UDP):** utilizado para el servicio DNS, que resuelve nombres de dominio en direcciones IP.

Problema identificado:

- El servicio DNS en el servidor 203.0.113.2 no está disponible en el puerto UDP 53. Esto impide que los clientes resuelvan la dirección IP del dominio yummyrecipesforme.com, provocando el error "puerto de destino inalcanzable".

Parte 2: Análisis de los datos y posibles causas del incidente

Parte 2: Análisis de los datos y posibles causas del incidente
Hora en que ocurrió el incidente: • Inicio del incidente: 13:24:32 • Persistencia del problema hasta: 13:28:50 **Cómo el equipo de TI se dio cuenta del incidente:** • Varias alertas de clientes reportando que no podían acceder al portal web. • Confirmación del error al intentar acceder al sitio web desde navegadores internos. **Acciones tomadas por el departamento de TI:** 1. Intento de acceso directo al sitio web para reproducir el error. 2. Captura del tráfico de red mediante **tcpdump** para registrar consultas DNS y respuestas ICMP. 3. Identificación de paquetes UDP destinados al puerto 53 y análisis de los mensajes ICMP de error recibidos. 4. Revisión preliminar de firewall y configuración del servidor DNS. **Hallazgos clave del análisis:** • Todas las solicitudes DNS enviadas al servidor fueron respondidas con ICMP de error "udp port 53 unreachable". • El puerto afectado es crítico para la resolución de nombres, lo que bloquea la navegación al dominio. • No se detectaron intentos de intrusión en los registros de red, lo que sugiere que la causa es un problema de disponibilidad del servicio y no necesariamente un ataque externo. **Posibles causas del incidente:** 1. **Firewall bloqueando el puerto UDP 53:** la configuración podría estar restringiendo tráfico DNS entrante. 2. **Fallo del servicio DNS en el servidor:** el demonio DNS podría estar caído o no iniciado. 3. **Problemas de red internos:** interrupciones en el enrutamiento o problemas de conectividad hacia el servidor DNS.

Solución propuesta y próximos pasos

1. **Verificación del firewall:** revisar reglas de entrada y salida para el puerto UDP 53, asegurando que el tráfico DNS no esté bloqueado.

2. **Revisión del servicio DNS:** confirmar que el demonio DNS está activo, reiniciarlo si es necesario y validar la resolución de nombres internamente.

3. **Pruebas de conectividad:** ejecutar `ping`, `traceroute` y `dig` para confirmar que los clientes pueden llegar al servidor DNS.

4. **Monitoreo de logs:** habilitar alertas y registro detallado de errores de DNS e ICMP para detectar problemas futuros.

5. **Documentación del incidente:** registrar los pasos tomados, hallazgos y medidas preventivas para referencia futura.

Presunta causa raíz:

- Servicio DNS inactivo o puerto UDP 53 bloqueado en el servidor, impidiendo la resolución de nombres de dominio.

Estado actual:

- El sitio web sigue inaccesible hasta que se validen los cambios en el firewall o se reinicie el servicio DNS.