**Informe de incidentes de ciberseguridad:**

**Análisis del tráfico de red**

|  |
| --- |
| Parte 1: Proporcione un resumen del problema encontrado en el DNS y el ICMP  registro de tráfico. |
| El protocolo UDP revela que:Puerto UDP 53 inalcanzable, longitud 254, en la cual se han realizado multiplies solicitudes hacia yummyrecipesforme.com. (24)  Esto se basa en los resultados del análisis de red, que muestran que la respuesta de eco ICMP devolvió el mensaje de error:Puerto UDP 53 inalcanzable, longitud 254  El puerto indicado en el mensaje de error se utiliza para:Cuando tu equipo intenta resolver la ip del dominio a traves de solicitudes dns, en este caso pregunta la ip de [yummyrecipesforme.com](http://yummyrecipesforme.com) asociada a 203.0.113.2 la cual mostraba error al intentarlo  El problema más probable es:Saturacion de solicitudes hacia una misma direccion |
|  |

|  |
| --- |
| Parte 2: Explique su análisis de los datos y proporcione al menos una causa del incidente. |
| Hora en que ocurrió el incidente:13:24:32.192571  Explique cómo el equipo de TI se enteró del incidente:En el momento de que unos de los usuarios intento ingresar hacia [yummyrecipesforme.com](http://yummyrecipesforme.com) pero le presentaba error de puerto inalcanzable, ademas el incidente ocurrió esta mañana cuando el equipo de recursos humanos (RR. HH.) informó que no podía acceder al portal web de verificación de antecedentes.  Explique las acciones tomadas por el departamento de TI para investigar el incidente:El equipo de seguridad de red respondió y comenzó a realizar pruebas con la herramienta de análisis de protocolos de red tcpdump. Los registros resultantes revelaron que el puerto 443, utilizado para el tráfico HTTPS, no es accesible. Seguimos investigando la causa del problema para determinar cómo podemos restaurar el acceso al portal web seguro. Nuestros próximos pasos incluyen verificar la configuración del firewall para ver si el puerto 443 está bloqueado y contactar al administrador del sistema del servidor web para que revise el sistema en busca de indicios de un ataque.  Tenga en cuenta los hallazgos clave de la investigación del departamento de TI (es decir, detalles relacionados con el puerto afectado, el servidor DNS, etc.):  Anote una posible causa del incidente:El equipo de RR. HH. cree que es posible que un nuevo empleado quiera impedir que se realice la verificación de antecedentes. El equipo de seguridad de red sospecha que esta persona podría haber lanzado un ataque para bloquear el sitio web de verificación de antecedentes. |

Aquí va un análisis claro y corto de ese tcpdump 👇

Resumen breve

* Tu host 192.51.100.15 envía consultas DNS (A) al servidor 203.0.113.2 usando UDP/53.
* El destino responde con ICMP “Destination unreachable – Port unreachable”: el puerto UDP 53 en 203.0.113.2 no está disponible.
* El patrón se repite varias veces: intentos de resolver yummyrecipesforme.com → rechazo por puerto inalcanzable → la resolución falla.

Protocolos observados

* IP
* UDP (servicio DNS, puerto destino 53, puerto origen efímero 52444)
* ICMP (tipo *Destination Unreachable*, código *Port Unreachable*)

Detalles del registro

* 192.51.100.15.52444 > 203.0.113.2.domain: ... A? yummyrecipesforme.com  
   → Consulta DNS tipo A desde un puerto efímero (52444) hacia DNS/53.
* 203.0.113.2 > 192.51.100.15: ICMP ... Puerto UDP 53 inalcanzable  
   → El equipo (o dispositivo en ruta) en 203.0.113.2 indica que no hay servicio escuchando en UDP/53 (o está bloqueado).

Interpretación de los problemas

1. Servidor DNS mal configurado o equivocado  
     
   * 203.0.113.0/24 es un bloque reservado para documentación/ejemplos; normalmente no debe usarse como DNS real.
   * Si lo usas, es normal obtener *port unreachable* o no obtener respuesta válida.
2. Firewall/ACL bloqueando UDP/53  
     
   * Si ese IP fuese tuyo interno, un firewall en el destino o intermedio puede estar rechazando el puerto 53.
3. Servicio DNS caído  
     
   * El proceso de DNS en ese host puede estar detenido o no escuchando en UDP.

Qué haría para solucionarlo (pasos rápidos)

Verifica el resolv.conf  
  
 cat /etc/resolv.conf

 Cambia el DNS a uno válido (por ejemplo 8.8.8.8 o tu DNS corporativo real):  
  
 sudo bash -c 'printf "nameserver 8.8.8.8\n" > /etc/resolv.conf'

Prueba resolución directa con dig  
  
 dig @8.8.8.8 yummyrecipesforme.com A

1. (Sustituye por tu DNS real si aplica.)
2. Si 203.0.113.2 es tu servidor

En el servidor: ¿está named/bind9/unbound corriendo?  
  
 sudo ss -lun | grep :53

sudo systemctl status bind9 unbound

Revisa firewall:  
  
 sudo iptables -S | grep 53

sudo ufw status

Captura focalizada para validar  
  
 sudo tcpdump -i eth0 '(udp port 53) or icmp'

Perfecto, Alberto 🚀  
 Con base en el registro de tcpdump que compartiste, te armo un informe estructurado de incidente de red:

Informe del Incidente de Red

1. Momento en que se informó del problema

El problema se detectó en el primer registro a las 13:24:32, cuando la IP 192.51.100.15 intentó resolver el dominio yummyrecipesforme.com enviando una consulta DNS (protocolo UDP, puerto 53) y recibió como respuesta un mensaje ICMP: Puerto UDP 53 inalcanzable desde 203.0.113.2.

2. Escenario, eventos y síntomas iniciales

* Escenario: Un cliente en la red (192.51.100.15) intenta realizar consultas DNS a un servidor (203.0.113.2).
* Eventos:  
    
  + El cliente envía consultas DNS repetidamente al puerto 53.
  + El servidor responde con ICMP de error: “Puerto UDP 53 inalcanzable”.
* Síntomas:  
    
  + Resolución de nombres fallida (no puede traducir yummyrecipesforme.com a una dirección IP).
  + Reintentos periódicos del cliente sin éxito.

3. Estado actual del problema

* El cliente sigue enviando consultas DNS a intervalos de aproximadamente un minuto.
* El servidor sigue rechazando las peticiones con ICMP.
* La resolución DNS no está funcionando, lo que afecta la navegación o conexión hacia dominios externos.

4. Información descubierta en la investigación

* Protocolos involucrados:  
    
  + UDP 53 (DNS) → usado para las consultas de resolución de nombres.
  + ICMP → utilizado por el servidor para notificar que el puerto 53 está cerrado o no disponible.
* El dominio solicitado: yummyrecipesforme.com.
* El problema persiste durante todo el rango de tiempo analizado (13:24 a 13:28).
* Esto puede deberse a:  
    
  + El servidor DNS en 203.0.113.2 no está ejecutando servicio en el puerto 53.
  + Restricción por firewall/bloqueo de tráfico DNS.
  + El cliente está intentando usar un servidor DNS incorrecto.

5. Próximos pasos para la resolución

1. Verificar conectividad: comprobar si 203.0.113.2 responde a ping o traceroute.
2. Validar servicio DNS: confirmar si el servidor DNS realmente escucha en el puerto 53 (nmap -p 53 203.0.113.2).
3. Revisar configuración del cliente: verificar qué servidor DNS está configurado en 192.51.100.15 (/etc/resolv.conf o configuración de red en Windows/Linux).
4. Probar resolución alternativa: usar un DNS público (ej. 8.8.8.8 o 1.1.1.1) para validar si el fallo es solo con 203.0.113.2.
5. Revisar firewall o IDS/IPS: confirmar que no haya reglas bloqueando tráfico DNS entre el cliente y el servidor.

6. Presunta causa raíz

El servidor DNS 203.0.113.2 no tiene el puerto UDP 53 disponible (cerrado o bloqueado), lo que provoca que todas las consultas de resolución de nombres del cliente fallen.  
 Esto podría deberse a:

* El servicio DNS no está en ejecución en ese servidor.
* El firewall en el servidor o en el camino bloquea el puerto 53.
* El cliente fue configurado con un DNS incorrecto.