# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that/El protocolo UDP revela que:  Utilizando el registro tcpdump para determinar que protocolo se estaba viendo perjudicado, se identificó que el *protocolo de mensajes de control de internet* es el que esta emitía el error.    Ocasionando que la página web yummyrecipesforme.com no esté operativa y nadie pudiera acceder a ella, esto se debe a un posible error de transmisión de datos.  Se evidencia que el error empieza a producirse sobre las 13:00hrs  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message/Esto se basa en que los resultados del análisis de red, el cual muestra que la respuesta de eco ICMP retorno con el mensaje de error:  "puerto de destino inalcanzable"    The port noted in the error message is used for/El puerto indicado en el mensaje de error es usado para:  Puerto 53 es usado normalmente para el servidor DNS.  The most likely issue is/El problema más probable es:  Esto puede indicar un problema de saturación de solicitudes en el servidor DNS, haciendo que este se bloquee es posible que sea un ataque malicioso de ataque de inundación ICMP. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred/Hora que ocurrio el indicente:  El incidente fue notificado al equipo de ciberseguridad entorno a las 13:00hrs.  Explain how the IT team became aware of the incident/Explique como el equipo de IT se dio cuenta del incidente:  El incidente fue reportado al equipo de seguridad por parte de varios clientes, comunicando que no podían acceder al sitio web de la empresa.    Explain the actions taken by the IT department to investigate the incident/Explique que acciones tomo el departamento de IT para investigar el incidente:  El equipo de seguridad respondió y comenzó a ejecutar pruebas con la herramienta de análisis de protocolo de red tcpdump, identificando así que el puerto 53 que normalmente es utilizado por el *protocolo de mensajes de control de internet* estaba siendo afectado.  Actualmente este incidente está siendo gestionado por ingenieros de seguridad después de que el equipo de seguridad y otros analistas hayan informado del problema a su supervisor directo.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.)/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.)/:  Los hallazgos claves en de la investigación reflejaron lo siguiente:  Puerto afectado: 53  Protocolo afectado: Protocolo de mensajes de internet  Servidor afectado: DNS  Hora de la prueba del incidente: 13:24hrs  IP origen: 203.0.113.2  IP destino: 192.51.100.15  Ataque: inundación ICMP  Mensaje de error: "puerto de destino inalcanzable"  Note a likely cause of the incident/Anote una causa probable del incidente:  Se sospecha que una persona podría haber lanzado el ataque para ser inaccesible para página web para los clientes. |