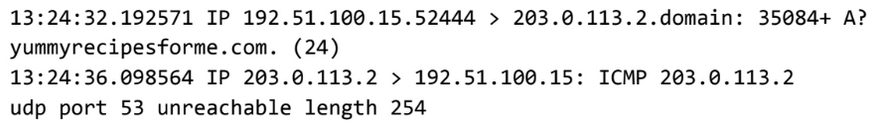
# Cybersecurity Incident Report:

# Network Traffic Analysis



| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| El protocolo UDP nos indica que la conexión no se ha podido realizar correctamente debido a un error como respuesta por parte del servidor. En este caso la conexión se realiza por el puerto UDP 53 y podemos recibir la cabecera del error “Unrecheable”.  Estamos ante un error ICMP que es el estándar entre dispositivos para comunicar errores en las conexiones. En este caso la conexión por parte del cliente 192.51.100.15 por el puerto 52444 es nula hacia la petición del dominio “yummyrecipesforme.com (203.0.113.2)”.  Esto nos indica probablemente que el dominio o IP que el cliente solicita conectarse no está disponible debido a un error en el web server o configuración del firewall. Podría tratarse perfectamente de un ataque de denegación de servicio o malware infectado dentro del servidor que responde a las peticiones. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| El incidente ocurrió a las 13:24 aproximadamente, el equipo de análisis de seguridad de la red recibió los reportes de varios usuarios que no podían acceder a la página web de la empresa cliente “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)”.  Una vez recibido el aviso, el equipo comenzó a realizar tareas de investigación usando herramientas como TCPdump para analizar los intentos de sesión y conexiones al servidor.  Localizada y desglosada la captura de la conexión y error, configuramos correctamente el firewall y lo revisamos para comprobar que todo funcione de manera correcta y solventar los posibles problemas por ese lado.  Una vez realizado el proceso de comprobación, contactamos con el administrador de la base de datos y página web para realizar un comprobación de los usuarios e intentos de sesión dentro de ambas partes.  Ahora sí, podemos ver un intento masivo de inicios de sesión junto con las peticiones relacionadas y confirmar que se trata de un ataque DOS.  Posibles soluciones:   * Monitoreo del tráfico a tiempo real. * Sistemas IDS. * Alertas automatizadas. |