**Escenario de acoso de la Universidad de Nitroba 2008**

Usted es un administrador de seguridad en la prestigiosa (y ficticia) Universidad Estatal de Nitroba.

El departamento de TI de Nitroba recibió un correo electrónico de Lily Tuckrige, profesora del Departamento de Química. Tuckrige ha estado recibiendo correos electrónicos de acoso y sospecha que están siendo enviados por un estudiante de su clase de Química 109, que está enseñando este verano. El correo electrónico fue recibido en la cuenta de correo electrónico personal de Tuckridge, lilytuckrige@yahoo.com. Tomó una captura de pantalla del navegador web y la envió.

El administrador del sistema que recibió la queja escribió a Tuckridge que Nitroba necesitaba los encabezados completos del mensaje de correo electrónico. Tuckridge respondió haciendo clic en el botón "Encabezados de mensajes completos" en Yahoo Mail y envió otra captura de pantalla, esta vez con encabezados de correo.

El encabezado del correo muestra que el mensaje de correo se originó en la dirección IP 140.247.62.34, que es un dormitorio de estudiantes de Nitroba. Tres mujeres comparten el dormitorio. Nitroba proporciona una conexión Ethernet en cada dormitorio, pero no acceso Wi-Fi, por lo que una de las amigas de las mujeres instaló un enrutador Wi-Fi en la habitación. No hay contraseña en el Wi-Fi.

Debido a que varios mensajes de correo electrónico parecen provenir de la dirección IP, Nitroba decide colocar un rastreador de red en el puerto ethernet. Todos los paquetes se registran. El lunes 7/21 Tuckridge recibió otro correo electrónico acosador. Pero esta vez, en lugar de recibirlo directamente, el perpetrador lo envió a través de un servicio basado en el sitio web llamado "willselfdestruct.com". El sitio web muestra brevemente el mensaje a Tuckridge, y luego el sitio web informa que el "mensaje ha sido destruido".

Se le han dado las capturas de pantalla, los paquetes que se recopilaron de la toma Ethernet y la lista Chem 109. Su trabajo es determinar si uno de los estudiantes de la clase fue responsable del correo electrónico de acoso y proporcionar evidencia clara y concluyente para respaldar su conclusión.

Los materiales didácticos para este escenario incluyen:

* Archivo pcap: alrededor de 60 MB
* Diapositivas que presentan el problema

Valores hash nitroba.pcap:

|  |  |
| --- | --- |
| **Algoritmo** | **Valor** |
| MD5 | 9981827f11968773ff815e39f5458ec8 |
| SHA1 | 65656392412add15f93f8585197a8998aaeb50a1 |
| SHA256 | 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb |

(Nota: Dado que los archivos de captura de paquetes contienen marcas de tiempo para cada paquete, este escenario debe tener una fecha y hora en que se lleva a cabo. Este escenario tiene lugar en el verano de 2008. Las marcas de fecha y hora no son relevantes para resolver el conjunto de problemas).