Escenario

En esta actividad, asumirás el papel de un analista de ciberseguridad que trabaja para una empresa que aloja el sitio web de cocina yummyrecipesforme.com. Los visitantes del sitio web experimentan un problema de seguridad al cargar la página web principal. Tu trabajo consiste en investigar, identificar, documentar y recomendar una solución al problema de seguridad.

Al investigar el evento de seguridad, revisarás un registro de tcpdump. Tendrás que identificar los protocolos de red utilizados para establecer la conexión entre el usuario y el sitio web. Los protocolos de red son las reglas y estándares de comunicación que los dispositivos en red utilizan para transmitir datos. Desafortunadamente, los actores maliciosos también pueden utilizar protocolos de red para invadir y atacar redes privadas. Saber identificar los protocolos utilizados habitualmente en los ataques te ayudará a proteger la red de tu organización contra este tipo de eventos de seguridad.

Para completar la tarea, también tendrás que documentar lo que ocurrió durante el incidente de seguridad. A continuación, recomendarás una medida de seguridad que se podría implementar para prevenir problemas de seguridad similares en el futuro.

Asegúrate de completar esta actividad antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo completo para compararlo con tu propio trabajo. No podrás acceder al modelo hasta que hayas finalizado esta actividad.