Contexto

Trabajas como analista de seguridad para una agencia de viajes que anuncia ventas y promociones en el sitio web de la empresa. Los empleados de la empresa acceden regularmente a la página web de ventas de la empresa para buscar paquetes vacacionales que puedan gustar a sus clientes. Una tarde, recibes una alerta automatizada de tu sistema de monitoreo que indica un problema con el servidor web. Intentas visitar el sitio web de la empresa, pero recibes un mensaje de error de tiempo de espera de conexión en tu navegador.

Utilizas un detector de paquetes para capturar los paquetes de datos en tránsito hacia y desde el servidor web. Observas un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida. El servidor web parece estar desbordado por el volumen de tráfico entrante y está perdiendo su capacidad para responder al número anormalmente grande de solicitudes SYN. Sospechas que el servidor está siendo atacado por un actor malicioso. Desconectas temporalmente el servidor para que el equipo pueda recuperarse y volver a un estado de funcionamiento normal. También configuras el firewall de la empresa para bloquear la dirección IP que estaba enviando el número anormal de solicitudes SYN.

Sabes que tu solución de bloqueo de IP no durará mucho, ya que un atacante puede suplantar otras direcciones IP para eludir este bloqueo. Tienes que alertar a tu gerente sobre este problema rápidamente y discutir los siguientes pasos para detener a este atacante y evitar que este problema vuelva a ocurrir. Tendrás que estar preparado para contarle a tu jefe el tipo de ataque que descubriste y cómo estaba afectando al servidor web y a los empleados.