Ejemplo de una

Informe de incidentes de ciberseguridad

Este **ejemplo de informe** corresponde a un evento de seguridad diferente al escenario presentado en la actividad. Este ejemplo solo debe utilizarse para familiarizarse con el formato de informe esperado.

| **Parte 1: Proporcione un resumen del problema encontrado en el registro de tráfico DNS e ICMP** | |
| --- | --- |
| Los registros del analizador de protocolo de red indican que no se puede acceder al puerto 443 cuando se intenta acceder al sitio web seguro de verificación de antecedentes de empleados. El puerto 443 se utiliza normalmente para el tráfico HTTPS. Esto puede indicar un problema con el servidor web o la configuración del firewall. Es posible que esto sea una indicación de un ataque malicioso al servidor web. | |
|

| **Parte 2: Explique su análisis de los datos y proporcione una solución para implementar** |
| --- |
| El incidente ocurrió esta mañana temprano cuando el equipo de recursos humanos (RR.HH.) informó que no podían acceder al portal web de verificación de antecedentes. El equipo de seguridad de la red respondió y comenzó a ejecutar pruebas con la herramienta de análisis de protocolo de red tcpdump. Los registros resultantes revelaron que el puerto 443, que se utiliza para el tráfico HTTPS, no es accesible. Seguimos investigando la causa raíz del problema para determinar cómo podemos restaurar el acceso al portal web seguro. Nuestros próximos pasos incluyen verificar la configuración del firewall para ver si el puerto 443 está bloqueado y contactar al administrador del sistema del servidor web para que verifique el sistema en busca de señales de un ataque. El equipo de RR.HH. cree que es posible que un nuevo empleado desee evitar que realice la verificación de antecedentes. El equipo de seguridad de la red sospecha que esta persona podría haber lanzado un ataque para bloquear el sitio web de verificación de antecedentes. |