**Sección 1: Identificar el protocolo de red involucrado en el incidente**

**¿Qué se hizo bien?**

1. **Identificación del protocolo HTTP**:
   * Si identificaste correctamente que el protocolo **HTTP** estaba involucrado en el incidente, esto demuestra que comprendes cómo funciona el tráfico web y cómo se relaciona con los servidores web.
   * Si mencionaste que el tráfico HTTP se utilizó para acceder al sitio web **yummyrecipesforme.com**, esto indica que puedes relacionar el protocolo con la actividad del usuario.
2. **Uso de herramientas de análisis**:
   * Si utilizaste **tcpdump** para capturar y analizar el tráfico de red, esto muestra que sabes cómo utilizar herramientas de red para diagnosticar problemas.

**¿En qué se puede mejorar?**

1. **Profundizar en la explicación del protocolo HTTP**:
   * Podrías haber explicado con más detalle cómo el protocolo HTTP funciona en la capa de aplicación y cómo se utiliza para transferir archivos maliciosos.
   * Falta mencionar que el protocolo HTTP es vulnerable a ataques como la inyección de código malicioso o la redirección a sitios web falsos.
2. **Mencionar otros protocolos involucrados**:
   * Aunque el HTTP fue el protocolo principal, podrías haber mencionado otros protocolos como **DNS** (para la resolución de nombres de dominio) o **TCP** (para establecer la conexión), ya que también están involucrados en el proceso de acceso a un sitio web.

**Sección 2: Documentar el incidente**

**¿Qué se hizo bien?**

1. **Descripción del incidente**:
   * Si describiste correctamente que los usuarios fueron redirigidos a un sitio web falso (**greatrecipesforme.com**) y se les solicitó descargar un archivo malicioso, esto demuestra que puedes identificar actividades sospechosas en la red.
   * Si mencionaste que el archivo malicioso comprometió los equipos de los usuarios, esto indica que comprendes el impacto de los ataques de ingeniería social.
2. **Uso de un entorno de pruebas (sandbox)**:
   * Si mencionaste que utilizaste un entorno de pruebas para analizar el sitio web sin afectar la red de la empresa, esto muestra que sabes cómo manejar situaciones de riesgo de manera segura.
3. **Análisis del código fuente**:
   * Si explicaste que el atacante manipuló el sitio web para agregar código malicioso, esto indica que puedes rastrear el origen del problema y entender cómo se llevó a cabo el ataque.

**¿En qué se puede mejorar?**

1. **Detalles sobre el ataque de fuerza bruta**:
   * Podrías haber proporcionado más detalles sobre cómo el atacante utilizó un ataque de **fuerza bruta** para acceder a la cuenta de administrador del sitio web. Por ejemplo, mencionar que el atacante probó múltiples combinaciones de contraseñas hasta encontrar la correcta.
   * Falta explicar cómo el ataque de fuerza bruta permitió al atacante cambiar la contraseña del administrador y tomar control del sitio web.
2. **Explicación más detallada del impacto**:
   * Podrías haber profundizado en cómo el archivo malicioso afectó a los equipos de los usuarios, mencionando que podría tratarse de un **malware** que ralentiza los sistemas o roba información.

**Sección 3: Recomendar una o más medidas de remediación para ataques de fuerza bruta**

**¿Qué se hizo bien?**

1. **Recomendación de medidas de seguridad**:
   * Si sugeriste implementar **autenticación de dos factores (2FA)**, esto demuestra que comprendes cómo esta medida puede prevenir ataques de fuerza bruta al requerir una segunda forma de autenticación.
   * Si mencionaste la importancia de **actualizar contraseñas con frecuencia** y **prohibir el uso de contraseñas anteriores**, esto indica que conoces buenas prácticas de seguridad para proteger cuentas de usuario.
2. **Explicación de las medidas**:
   * Si explicaste cómo el 2FA requiere un código de un solo uso (OTP) enviado al correo o teléfono del usuario, esto muestra que puedes comunicar claramente las medidas de seguridad.

**¿En qué se puede mejorar?**

1. **Profundizar en las medidas de seguridad**:
   * Podrías haber mencionado otras medidas de seguridad, como la implementación de **límites de intentos de inicio de sesión** para bloquear cuentas después de varios intentos fallidos, o el uso de **CAPTCHA** para prevenir ataques automatizados.
   * Falta explicar cómo estas medidas podrían integrarse en la infraestructura actual de la organización.
2. **Mencionar la importancia de la educación del usuario**:
   * Podrías haber sugerido la implementación de **programas de concienciación sobre seguridad** para educar a los usuarios sobre cómo identificar y evitar descargar archivos maliciosos.

**Conclusión**

**¿Qué se hizo bien?**

* Identificaste correctamente el protocolo HTTP involucrado en el incidente.
* Documentaste el incidente de manera clara, incluyendo la redirección a un sitio web falso y la descarga de un archivo malicioso.
* Recomendaste medidas de seguridad efectivas, como la autenticación de dos factores y la actualización frecuente de contraseñas.

**¿En qué se puede mejorar?**

* Profundizar en la explicación técnica del protocolo HTTP y su vulnerabilidad a ataques.
* Proporcionar más detalles sobre el ataque de fuerza bruta y cómo se llevó a cabo.
* Sugerir medidas adicionales de seguridad, como límites de intentos de inicio de sesión y programas de concienciación para usuarios.
* Mejorar la claridad y estructura del informe para que sea más fácil de seguir.

**Puntos clave para seguir avanzando en el curso**

1. **Practica el análisis de tráfico de red**:
   * Sigue trabajando con herramientas como **tcpdump** o **Wireshark** para analizar tráfico de red y familiarizarte con los diferentes tipos de ataques.
2. **Amplía tus conocimientos sobre protocolos de red**:
   * Aprende más sobre cómo funcionan los protocolos como HTTP, DNS, y TCP, y cómo pueden ser explotados por atacantes.
3. **Profundiza en la seguridad de red**:
   * Investiga más sobre cómo prevenir ataques de fuerza bruta, como la implementación de CAPTCHA, límites de intentos de inicio de sesión, y sistemas de detección de intrusiones (IDS).
4. **Mejora tus habilidades de redacción**:
   * Practica la escritura de informes técnicos claros y concisos, asegurándote de que cada sección esté bien estructurada y fácil de entender.

**Nota final**

El ejemplar representa una posible explicación de los problemas a los que se enfrentan los usuarios finales. Es probable que tu análisis difiera en ciertos aspectos, pero lo importante es que hayas identificado los protocolos de red implicados y hayas creado un informe coherente. Como analista de seguridad, es fundamental documentar cualquier problema que ocurra en la red y proponer sol

Cuanta más práctica tengas en la identificación de patrones en los registros y datos, más fácil te resultará detectar los ataques a la red en el momento en que se producen. Esto te permitirá responder a los incidentes con mayor rapidez y eficacia.