Actividad 02. Seguridad en conexiones inalámbricas

1. Realiza un documento sobre la seguridad en redes inalámbricas

Las redes inalámbricas han revolucionado la manera de conectarnos y compartirnos información, dando flexibilidad y conveniencia tanto en entornos domésticos como empresariales. Sin embargo, esto viene acompañado de riesgos de seguridad inherentes a la naturaleza abierta de las señales inalámbricas. Proteger la red inalámbrica implica no sólo conocer las amenazas potenciales, sino implementar estrategias efectivas de mitigación.

Sus principales amenazas son las siguientes y que hay que evitar:

1. ***INTERCEPCIÓN DE TRÁFICO (SNIFFING)***:
    - **Descripción**: La intercepción de tráfico o *sniffing* es una técnica utilizada por los atacantes para capturar y analizar los paquetes de datos que circulan en la red. Este tipo de ataque es bastante peligroso en redes que no emplean cifrado adecuado, ya que permite que el atacante pueda acceder a la información sensible (credenciales de usuario, correo electrónico y/o datos confidenciales).
    - **Prevención**: Utilizar cifrado de alta calidad (WPA3), que asegura que los datos transmitidos estén protegidos incluso si son interceptados. Además, evitar el uso de redes inalámbricas abiertas o públicas sin protección es crucial.
2. ***ACCESO NO AUTORIZADO***:
    - **Descripción**: El acceso no autorizado ocurre cuando un usuario no identificado se conecta a la red sin permiso, permitiéndole acceder a la información sensible o para usar los recursos de la red para lanzar otros ataques. Puede resultar en el robo de

información, la instalación de malware o la interrupción de servicios.
    - **Prevención**: Implementar contraseñas complejas y únicas, además de utilizar autenticación multifactor (MFA). Limitar el acceso mediante la identificación de direcciones MAC y la creación de listas blancas también puede ayudar a controlar qué dispositivos pueden conectarse a la red.
3. ***ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)***:
    - **Descripción**: Los ataques de denegación de servicio tienen como objetivo sobrecargar la red en un exceso de tráfico, lo que resulta en la interrupción de los servicios legítimos. En el contexto de redes inalámbricas, estos ataques pueden dejar a los usuarios sin acceso a Internet o a recursos críticos de la red.
    - **Prevención**: Implementar soluciones de mitigación de DoS (sistemas de detección de intrusos [IDS]) que identifiquen y bloqueen el tráfico anómalo. Además, la configuración adecuada de puntos de acceso para manejar grandes volúmenes de tráfico y la segmentación de la red pueden ayudar a reducir el impacto de estos ataques.
4. ***ROGUE ACCESS POINTS (PUNTOS DE ACCESO FALSOS)***:
    - **Descripción**: Los puntos de acceso falsos son dispositivos configurados para imitar a los puntos de acceso legítimos de la red, engañando a los usuarios para que se conecten a ellos. Una vez conectados, los atacantes pueden capturar información sensible o inyectar malware en los dispositivos.
    - **Prevención**: El monitoreo constante de la red para identificar dispositivos no autorizados es fundamental. Los sistemas de gestión de red inalámbrica son buenas herramientas para detectar estos puntos de acceso falsos y alertar a los administradores para que se tome la acción.
5. ***SPOOFING***:
    - **Descripción**: El *spoofing* es la suplantación de identidad, donde el atacante manipula direcciones IP, MAC u otros identificadores para hacerse pasar por un dispositivo legítimo de la red. Puede permitir al atacante acceder a la información confidencial o causar conflictos en la red.
    - **Prevención**: Utilizar cifrado robusto (WPA3 y técnicas de autenticación seguras). También es recomendable habilitar el cifrado de MAC y emplear herramientas de detección de anomalías en la red.

6. ***MAN-IN-THE-MIDDLE (MitM)***:
    - **Descripción**: Los ataques Man-in-the-Middle (MintM) ocurren cuando un atacante intercepta y manipula la comunicación entre dos partes sin que ninguna de ellas lo sepa. Permite al intruso leer, modificar e insertar mensajes maliciosos en la comunicación.
    - **Prevención**: Utilizar protocolos de comunicación seguros (HTTPS, SSL/TLS y redes privadas virtuales [VPN]). Además, educar a los usuarios sobre los riesgos de las redes inalámbricas abiertas y la importancia de verificar certificados de seguridad también es crucial.

Hay que hacer buenas prácticas de seguridad en Redes Inalámbricas, algunas de estas buenas prácticas son:

1. ***CIFRADO AVANZADO***:
    - **WPA3**: El estándar más reciente en seguridad inalámbrica ofrece un cifrado más robusto y protege mejor contra ataques de fuerza bruta. Recomendable actualizar todos los dispositivos de la red para que sean compatibles con el estándar.
    - **WPA2**: Sigue siendo opción válida si WPA3 no está disponible. Es importante asegurarse de que esté configurado correctamente, utilizando una clave de cifrado fuerte.
2. ***AUTENTICACIÓN FUERTE***:
    - **Autenticación Multifactor (MFA)**: Implementar MFA añade una capa adicional de seguridad, requiriendo no sólo la contraseña, sino un segundo factor (aplicación de autenticación o dispositivo biométrico), para verificar la identidad del usuario.
    - **Políticas de Contraseñas**: Establecer políticas estrictas que requieran contraseñas largas, complejas y que se cambien periódicamente ayuda a prevenir accesos no autorizados.
3. ***MONITOREO CONTINUO***:
    - **Sistemas de Detección de Intrusos (IDS)**: Los IDS son herramientas que monitorizan la red en busca de actividades sospechosas o no autorizadas. Configurar alertas y revisar regularmente los registros de eventos es esencial para una respuesta rápida ante incidentes de seguridad.

- **Análisis de Tráfico**: Realizar análisis periódicos del tráfico de la red puede ayudar a identificar patrones anómalos que podrían indicar un intento de ataque.

4. ***SEGMENTACIÓN DE RED***:
   - **Segmentación por VLAN**: Dividir la red en subredes o VLANs puede limitar el alcance del ataque, impidiendo que un intruso tenga acceso a toda la red si compromete un sólo dispositivo.
   - **Redes Invitadas**: Establecer redes separadas para invitados o dispositivos no confiables reduce el riesgo de que éstos comprometan la red principal
5. ***ACTUALIZACIONES REGULARES***:
   - **Parches de Seguridad**: Mantener todos los dispositivos, incluyendo routers y puntos de acceso, actualizados con los últimos parches de seguridad para proteger la red contra vulnerabilidades conocidas.
   - **Firmware y Software**: Asegurarse que el firmware de los dispositivos de red esté actualizado y que el software de seguridad (antivirus y firewalls) esté configurado correctamente.

En definitiva, la seguridad en redes inalámbricas es un desafío continuo que requiere una combinación de tecnología avanzada y buenas prácticas. Al comprender las amenazas y aplicar las estrategias de protección adecuadas, las organizaciones pueden reducir los riesgos asociados con el uso de redes inalámbricas. Es esencial mantener una postura proactiva y adaptarse continuamente a las nuevas amenazas y soluciones que surgen en el panorama de la ciberseguridad.