SIFI WSS

ID : 1

BSSID : 0C-B9-37-4A-F8-CC

ESSID : NETBEDROOM

Agente SIFI : 100.64.0.4

El handshake capturado es : handshake_NETBEDROOM_0C-B9-37-4A-F8-CC_2022-04-19T07-18-21.cap

Contraseña del AP : 123456

Tipo de test realizado: WPA/WPA2 Advance

Sifi Score:

Segun el assesment de la red, la puntuacion asignada es:

Sifi Score: Vulnerable. La red pudo ser vulnerada en al menos dos ambitos.

RECOMENDACIONES

A parte de haber capturado el 4-full way handshake, se pudo hacer un crack de la contraseña

Segun el libro CWSP en su capitulo 9.1.8 se recomienda actualizar a una solución de autenticación 802.1X/EAP usando autenticación tunelada.

Mejores practicas a tomar

- Política corporativa: Un apéndice adicional a las recomendaciones de seguridad podrían ser las recomendaciones de políticas WLAN corporativas. El auditor puede ayudar al cliente a redactar una política de seguridad de la red inalámbrica si aún no tiene una.
- Seguridad física: La instalación de unidades de cerramiento para proteger contra el robo y el acceso físico no autorizado a los puntos de acceso puede ser una recomendación. Estas también se utilizan a menudo con fines estéticos.

Directrices de contraseñas PCI-DSS

Su contraseña no tiene caracteres especiales por lo tanto presentamos tecnicas de se deben tener en cuenta:

Segun la guia de PCI-DSS en la seccion 4.4 se plantean las siguientes recomendaciones para mas seguridad:

- Se debe cambiar siempre los valores predeterminados que fueron proporcionados por el proveedor, esto incluye las contraseñas y las configuraciones como tambien deshabilitar las cuentas innecesarias antes de instalar su propio sistema de red.
- Eliminar o deshabilitar cuentas de usuarios inactivas dentro de 90 dias
- Limitar los intentos de acceso repetidos bloqueando el ID de usuario despues de mas de 5 intentos y establecer una duracion de bloqueo en un minimo de 30 minutos o hasta que el administrador habilite el ID del usuario.
- Se debe cambiar la contraseña de los usuarios una vez cada 90 dias y no permitir que se repita las ultimas cuatro contraseñas.
- Establecer contraseñas para el primer uso y al restablecerlas a un valor unico para cada usuario y cambiar inmediatamente despues del primer uso. Hacer cumplir la autenticacion multifactor

Directrices de contraseñas PCI-DSS

Su contraseña no posee la longitud recomendada, por lo tanto presentamos tecnicas de se deben tener en cuenta

Segun la guia de PCI-DSS en la seccion 4.4 se plantean las siguientes recomendaciones para mas seguridad:

- Se debe cambiar siempre los valores predeterminados que fueron proporcionados por el proveedor, esto incluye las contraseñas y las configuraciones como tambien deshabilitar las cuentas innecesarias antes de instalar su propio sistema de red.
- Eliminar o deshabilitar cuentas de usuarios inactivas dentro de 90 dias
- Limitar los intentos de acceso repetidos bloqueando el ID de usuario despues de mas de 5 intentos y establecer una duracion de bloqueo en un minimo de 30 minutos o hasta que el administrador habilite el ID del usuario.
- Se debe cambiar la contraseña de los usuarios una vez cada 90 dias y no permitir que se repita las ultimas cuatro contraseñas.
- Establecer contraseñas para el primer uso y al restablecerlas a un valor unico para cada usuario y cambiar inmediatamente despues del primer uso. Hacer cumplir la autenticacion multifactor