Ciberseguridad Cuestionario sobre protocolo SSH

Respuestas:

Sección 1:

1. B, La principal función del protocolo SSH es permitir el acceso remoto a los servidores para ejecutar scripts entre otras cosas, además cuenta con una conexión al servidor cifrado la cual garantiza la confidencialidad e integridad de los datos.

2. B, Actualmente se recomienda la versión SSHv2 porque la versión SSHv1 ya no se considera segura ya que tiene vulnerabilidades conocidas por ende quedó obsoleta para los ataques actuales.

3. B, para evitar escaneos de bots que siempre están direccionados al puerto 22 (ósea SSH) se recomienda cambiar el puerto para que tome más trabajo encontrar el puerto y una vez encuentren el puerto recién puedan empezar a hacer algo.

Sección 2:

4. Verdadero, un usuario con poca experiencia en consolas de comandos puede frustrarse ante el hecho de tener que configurar todo en una interfaz anticuada si estás acostumbrado a una interfaz gráfica tipo windows, ademas por mas que para algunos usuarios experimentados parezca fácil, tiene sus mañas y hasta no conocerlas te la pegas contra la pared varias veces como principiante.

5. Verdadero, y es recomendable, porque usualmente los bots intentan conectarse al puerto 22 y con el usuario root, entonces si les cambiamos el usuario, además de conectarse van a tener que adivinar el nombre del usuario, se puede deshabilitar modificando el archivo sshd_config y poniendo PermitRootLogin no.

6. Verdadero, SSH utiliza varios protocolos para esto, entre ellos utiliza cifrado simétrico, el cual usa una llave secreta para descifrar un mensaje, cifrado asimétrico, que son dos llaves separadas, una para cifrar y otra para descifrar y el Hashing que son códigos unidireccionales, por ejemplo hola puede ser hasheado y quedar como 21xss214515 y que holaa sea 9jjjjjjsw672sb (nada que ver y eso que solo agregamos una letra) por eso son unidireccionales, además de autentificar la identidad de las personas que intentan ingresar mediante la HMAC que es como la cédula de nuestro router.

Sección 3:

7. Antes que nada, mantener el software actualizado es de vital importancia, las actualizaciones muchas veces incluyen mejoras de seguridad sobre vulnerabilidades recientes y corrección de errores. Otra es usar contraseñas seguras, porque podes poner toda la seguridad que quieras en los programas pero si tu contraseña no es segura puede ser vulnerada fácilmente ya que existen archivos enormes con contraseñas muy utilizadas que en cuestión de horas descifran la tuya. Limitar el acceso de las direcciones IP que se pueden conectar es de gran utilidad, por ejemplo usando el proyecto, en el software de gestión de cooperativas, para mayor seguridad nos conviene bloquear ips que no sean de Uruguay, porque va a ser un programa exclusivamente utilizado en el país. Por más que estas medidas parecen simples, reducen el riesgo de accesos no autorizados brutalmente.

8. Los 2 métodos principales son Usuario y contrase;a o clave pública, el usuario y contrase;a es a lo que acostumbramos siempre, para establecerlo es necesario que lo habilitemos en el archivo de configuración y al intentar conectarse al server te pide usuario y contrase;a, pero es vulnerables a ataques de fuerza bruta o contraseñas comunes. Por otro lado están las claves públicas que también se tiene que activar el uso en el archivo de configuración y lo que se hace es que el usuario genera en su compu una clave privada que se guarda localmente y una pública que se guarda una copia en el server. Una vez se configura el usuario, el puede entrar sin pasar por ningún login ni nada, se autentifica usando la clave.

9. La autenticación con clave pública es bastante más segura porque elimina el riesgo de ataques de fuerza bruta y no transmite contraseñas por la red, Como dice en el documento "*disponer de claves SSH es sinónimo de los más altos niveles de seguridad en comparación con las contraseñas*". Además de que se puede configurar para que solo se pueda ingresar con llave pública y que cualquier intento de login sea automáticamente rechazado a menos que sea el del usuario con la llave.

10. Dos de las herramientas que menciona el documento para verificar si la configuración que hicimos es segura son, Rebex SSH Check y ssh-audit, las dos evalúan la seguridad del servidor de distintas maneras, Rebex SSH Check es una herramienta online que analiza nuestro server SSH y muestra los algoritmos de cifrado, intercambio de claves y MAC que estemos usando. También resalta si algo está inseguro o obsoleto, por otro lado esta ssh-audit que es un script escrito en Python, hecho para ejecutarse en el servidor, el cual realiza un escaneo completo de la configuración y genera un informe detallado de los parámetros inseguros o vulnerables.