**TeamREG**

**Integrantes:**

Gilberto Morales Medina 2098206

Roel Antonio Guzman Martinez 2066072

Emiliano Villarreal Saracco 2033644

**¿Qué se considera una contraseña débil?**

Es una contraseña corta, predecibles, o que tenga palabras del diccionario, información personas como tu fecha de nacimiento, tu nombre, o el de una mascota, o teclas que van seguías como el qwerty o 123456.

**¿Qué características debe tener una contraseña fuerte?**

Debe ser suficientemente larga, con 12 caracteres o 16, también debe ser compleja (con mayúsculas, números, y símbolos), igualmente debe ser única, no debe ser usada en otras plataformas.

**¿Qué riesgos existen al usar contraseñas débiles?**

Pues pueden robar tu identidad, pueden acceder a datos personales o sensibles sin autorización, perder dinero, y si se trata de una empresa, se puede dañar la reputación de la empresa.

**¿Cómo puedes asegurarte de que tu trabajo como auditor fortalezca la seguridad en lugar de debilitarla?**

Actuando siempre con un permiso muy específico, definiendo claramente hasta dónde puedo llegar, manteniendo la confidencialidad y reportando las vulnerabilidades de forma responsable para que sean corregidas.

**Si una contraseña fuerte protege la información, pero los usuarios suelen olvidarlas, ¿cómo equilibrar la seguridad con la usabilidad?**

Por medio de gestores de contraseñas, la implementación obligatoria de Autenticación de Múltiples Factores (MFA) y fomentando el uso de "frases de contraseña" que son más fáciles de recordar.

**¿Qué es más peligroso: una contraseña débil o un usuario que la anota en un post-it pegado al monitor?**

El post-it, porque es una vulnerabilidad física que expone la contraseña, aún si es fuerte, porque cualquier persona la puede ver, saltándose todas las defensas digitales.

**¿Cuál es la línea que separa una auditoría ética de un ataque malicioso?**

El permiso y la intención, el auditor tiene autorización para encontrar fallos con el fin de mejorar la seguridad, pero el atacante no tiene permiso y busca explotar los fallos para su beneficio.

**¿Qué principios deberían guiar tu práctica profesional cuando usas herramientas como john o diccionarios de contraseñas?**

Legalidad, Consentimiento, Confidencialidad y Reporte Responsable. Siempre se debe actuar dentro de un marco ético y profesional.

**¿Qué implicaciones tiene clasificar contraseñas como “fuertes” solo porque john no las descifró?**

Significa que es fuerte contra ese diccionario específico, puede ser vulnerable a otros diccionarios, a ataques de fuerza bruta o a otras técnicas.

**¿Podría esto generar una falsa sensación de seguridad en la organización?**

Sí, en el informe se debe explicar que la prueba tiene limitaciones y que "fuerte" no significa que sea indescifrable.

**Si tu reporte fuera leído por un directivo sin conocimientos técnicos, ¿cómo lo explicarías para que entienda la gravedad de usar contraseñas débiles sin exponer información sensible?**

Yo usaría como una analogía, le explicaría que tener contraseñas débiles es como poner una puerta para que no entre nadie, pero que está cerrada con un candado de diario, los atacantes no intentarán romper la puerta, simplemente abrirán el candado fácil y entrarán.

**¿Qué recomendación práctica le darías a una organización que depende todavía de contraseñas tradicionales?**

El implementar MFA, esta es la medida más efectiva, también el promover el uso de gestores de contraseñas en toda la empresa, también establecer una política de contraseñas robusta que exija que sean largas y complejas, y finalmente el hacer capacitaciones continuas sobre phishing y seguridad.