Sombreros Negros vs Sombreros Blancos

Esta ***WebQuest*** está dirigida al alumnado de **Bachillerato**. Para responder las preguntas que encontrarás más abajo, deberás de consultar la siguiente web. Pincha en el enlace que encontrarás a continuación:

https://edea.juntadeandalucia.es/bancorecursos/file/739d282a-a89b-4db4-818d-8bc3f06265bc/2/CDI_1BACH_REA_01_V02.zip/index.html

El objetivo a conseguir en esta ***WebQuest*** será que puedas contestar a las siguientes preguntas:

1. ¿Qué **tipos de ataques** informáticos existen?
2. ¿Cuál es la diferencia entre **hacking** y **hacking ético**?
3. ¿Cuántos tipos de **hackers** hay?
4. ¿Qué **técnicas de búsqueda** de información utilizan?
5. ¿Cuáles son las **vulnerabilidades** utilizadas por los hackers en un sistema informático?
6. ¿Qué **repercusiones legales** tienen estos delitos?
7. ¿Qué **técnicas de protección** deben emplear?
8. ¿Cómo pueden implementarse en la empresa?
9. ¿Cómo puede una empresa mantener seguros sus **datos**?
10. ¿Cómo debe actuar en caso de un ataque?

Deberás responder en tu cuaderno a las siguientes preguntas, buscando las respuestas en la web del inicio de este documento:

1. Presentación.

a). Escribe la definición de *hackers y crakers.*
b). Visualiza el video *Introducción a la ciberseguridad* y escribe en tu trabajo las ideas más importantes.

2. Víctimas de un ciberataque.

a). Realiza la actividad del apartado *Tu vocabulario de ciberseguridad*.

3. Contraseñas y antivirus.

a). ¿Cuál es Según el *Instituto Nacional de Ciberseguridad* uno de los errores más habituales que cometen los usuarios en la gestión de las contraseñas?

3.1. Tu contraseña no es segura.

a). Escribe los consejos a seguir para crear contraseñas seguras.
b). Explica que debemos hacer para gestionar nuestras contraseñas.
c). ¿Qué podría pasar si alguien consigue tus contraseñas?
d). Escribe los consejos y recomendaciones para crear una contraseña fuerte.
e). Realiza la actividad *Adivina mi contraseña.*
f). ¿Qué permite un *gestor de contraseñas?*
g). ¿Qué es un *plugin?*

3.2.Virus, troyanos y gusanos.

a). ¿Qué es un *spyware?*
b). Explica las diferencias entre *virus, troyanos y gusanos.*
c). ¿Qué son los *ataques de día cero*?
d). ¿Cuáles deben ser las características más importantes?
e). Enumera los consejos para escoger un buen antivirus

4. Quiero ser un hacker.

a). ¿Cómo se llaman los hackers buenos y malos*?* ¿A qué se dedican?
b). ¿Quiénes son los *hackers de sombrero gris*?
c). Realiza la actividad del apartado *¿Qué tipo de hacker te gustaría ser?*

4.1. Hacking ético.

a). ¿Qué entendemos como *hacking ético?*
b). ¿Cuál es el objetivo de los *test de penetración*? Visualiza el video y escribe las ideas principales.
c). Realiza la actividad *Comprueba lo que sabes.*

4.2. Tipos de ataque.

a). Escribe la clasificación de los tipos de ataque y sus principales ataques de cada uno.

b). Realiza la actividad *Tipos de ataques más comunes.*

5. Técnicas de Pentesting.

a). ¿Qué es el *Pentesting?*

5.1. Técnicas de búsqueda de información.

a). ¿Qué entendemos como *Information gathering?* ¿Qué fases tiene?
b). ¿Qué es *Whois*?
c). ¿Qué es *Tracert*? ¿Para qué sirve?
d). ¿Qué es el comando *Ping*? ¿Cómo se ejecuta?
e). Explica brevemente en que consisten los protocolos *SSL* y *TLS*.
f). Realiza la actividad *Pon a prueba tus conocimientos.*

5.2. Pruebas de Pentesting.

a). Escribe las fases de *Pentesting* que existen.
b). Explica cuales son los tipos y objetivos del *Pentesting*.
c). Realiza la actividad *Tienes los conceptos claros.*

6. Vulnerabilidades en sistemas.

6.1. Ingeniería social.

a). Realiza la actividad *Actúa como un hacker*.

6.2. Atacamos un equipo.

a). ¿Qué es el *Kali Linux*? ¿Para qué está diseñado?
b). ¿Qué es un *exploit*? ¿Qué pueden proporcionar?

6.3. Análisis de riesgos.

a). ¿Qué tipo de amenazas existen? Explícalas.
b). ¿Cuáles son las medidas de protección más importantes?
c). ¿Qué son las contramedidas? ¿Qué técnicas y herramientas se utilizan?
d). Realiza la actividad *¿Cómo lo hago?*

7. Análisis forense.

a). ¿Qué es la informática forense? ¿Qué casos se investigan?
b). Realiza la actividad *Responde a estas cuestiones.*

8. Ciberdelitos.

a). ¿Qué es la ciberdelincuencia?
b). Escribe las características mas importantes de la *ley NIS*.
c). ¿Cuáles son las consecuencias de los delitos informáticos?