SGSSI-20.HA1.Test.18.JDOR

A.2.2.2

1. ¿Cuantos euros de multa tuvo que pagar L. J. M. D? (el primer delincuente mencionado en el texto)

1. 20.000 (Veinte mil)
2. 200.000 (Doscientos mil)
3. 2.000 (Dos mil)
4. 35.000 (Treintaicinco mil)

2. ¿Cual es el texto original detrás del del texto MJQQT, ejemplo del vídeo, mediante el cifrado de César?

1. COFFE
2. THINK
3. HELLO
4. THING

3. ¿Qué otra medida de seguridad se toma en el nivel 3 de Google además de la tarjeta identificadora?

1. Escáner dactilar
2. Todas las opciones son incorrectas
3. Se necesita una contraseña predeterminada
4. Escáner de iris

4. La longitud de un Hash

1. Puede variar según la longitud de documento
2. Es siempre diferente
3. Es siempre la misma
4. Depende de los movimientos relacionados con el ratón

A.4.1.3

1. Según el documento "*¿Qué debo saber sobre el cifrado?"* ¿Cual es el ataque mencionado que afecta a la memoria RAM?

1. Cold Boot Attack
2. MITM (Man In The Middle)
3. Phishing
4. Stack Overflow

2. Según el documento "*¿Qué debo saber sobre el cifrado?"* ¿Cual es la extension recomendada en el apartado de cifrado por capas de transporte?

1. Ublock Origin
2. Privacy Badger
3. HTTPS Everywhere
4. Dark Reader

3. Según el documento "*¿Qué debo saber sobre el cifrado?"* El cifrado de la capa de transporte es conocido por sus siglas en inglés que son...

1. TLS
2. ISP
3. VPN
4. HTTPS

4. Según el documento "*¿Qué debo saber sobre el cifrado?"* ¿Cual es el metodo de crifrado para mensajeria instantanea mencionada?

1. PGP
2. OTR
3. GPG
4. AES

A.5.1.3

1. Según el video “Transport Layer Security - Applied Cryptography” el TLS Handshake protocol estable los siguiente pasos:
    1. Autenticacion, establecer los protocolos de cifrado y establecer una clave de sesion
    2. Autenticacion y establecer los protocolos de cifrado
    3. Autenticacion, trazabilizar al cliente y establecer una clave de sesion
    4. Establecer los protocolos de cifrado y establecer una clave de sesion

2. Según el video “Lección 9: Introducción al protocolo SSL (intypedia)” el cifrado Asimetrico se utiliza para...
    1. No se utiliza para nada, todo es simetrico
    2. Toda la comunicacion se cifra asimetricamente
    3. Intercambio de claves y firma
    4. Solo para firmar

3. Según el video “Bitcoin - Transaction records” especifica sobre las transacciones realizadas...
    1. Que son guardadas y almacenadas de modo que un bitcoin guarda la informacion de todos sus “dueños”
    2. Que solo almacena el ultimo por si ha habido algun error
    3. Que no almacena este tipo de informacion, son “amnesicos”
    4. Que solo lo almacena durante un periodo de tiempo establecido en la transaccion

4. Según el video “Bitcoin - Proof of work” el primer uso (cronologico) que menciona el autor es...
    1. Bitcoin
    2. Separar el SPAM del correo
    3. Ataques tipo DoS
    4. Codigos Captcha

A.2.2.2

1. Correcta: A (20.000 (Veinte mil)) [Párrafo 6, penúltima línea]
2. Correcta: C (HELLO) [Minuto 1:39 del vídeo]
3. Correcta: D (Escáner de iris) [Minuto 2:33 del vídeo]
4. Correcta: C (Es siempre la misma) [Minuto 2:19 del vídeo]

A.4.1.3

1. Correcta: 1 (Cold Boot Attack, bastante al inicio del apartado “Cifrado de datos en reposo”)
2. Correcta: 3 (HTTPS Everywhere, en el ejemplo sobre HTTPS)
3. Correcta: 1 (TLS, Transport Layer Security o Seguridad de la capa de transporte)
4. Correcta: 2 (OTR, Lo menciona justo en parrafo superior al GIF)

A.5.1.3

1. Correcta: 1 Autenticacion, establecer los protocolos de cifrado y establecer una clave de sesion (min 1:00 del video)
2. Correcta: 3 Intercambio de claves y firma (min 7:23)
3. Correcta: 1 Es guardada y almacenada de modo que un bitcoin guarda la informacion de todos sus “dueños” (min 4:06)
4. Correcta: 2 (min 1:51)