|  |  |
| --- | --- |
| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| Nombre de la actividad | Seguridad digital |
| Objetivo de la actividad | Reconocer las diferentes formas de ataque en redes IoT y sus posibles soluciones. |
| Tipo de actividad sugerida | Falso-Verdadero |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo1\_CF01\_ActividadDidáctica |

**INSTRUCCIONES PARA EL APRENDIZ**

Apreciado participante a continuación encontrará una actividad didáctica, para afianzar los conceptos y aprendizajes del componente de formación.

Lea las situaciones y marque como falso o verdadero la formulación a la cual corresponde:

1. MQTT se basa en el principio de publicación de mensajes y suscripción a los temas.

R/ verdadero

1. Nunca debo usar TLS con MQTT.

R/Falso

1. La encriptación asimétrica se basa en la codificación de la información basada en dos claves.

R/ verdadero

1. El protocolo MQTT puede ser atacado con ataques mediante MQTT malaria.

R/ verdadero

1. El protocolo MQTT pertenece a la capa de aplicación y trabaja sobre el protocolo TCP.

R/ verdadero

1. El protocolo MQTT usa el modelo de PUBLICAR / SUSCRIBIR.

R/ verdadero

**Retroalimentación:**

1. El protocolo MQTT es un protocolo de conectividad M2M, es liviano permitiendo el modelo de mensajería publicación/suscripción.
2. Se debe asegurar la comunicación confiable entre cliente y servidor usando TLS, evitando que un atacante pueda interceptar la comunicación.
3. La codificación asimétrica se basa en:

**Clave pública:** permite encriptar mensajes que solo se cifran con la clave privada.

**Clave privada:** permite descifrar los mensajes cifrados por la clave pública, siempre y cuando se cuente con la clave pública.

1. El ataque está basado en MOSQUITTO, simulando varios clientes, publicando mensajes de tamaños grandes y enviando a grandes velocidades.
2. MQTT se basa en conexiones TCP IP y utiliza el puerto .1883 reservado por la IANA (Assigned Numbers Authority).
3. Se originan mensajes de publicación /suscripción que proporcionan la distribución de uno a varias aplicaciones.

**Correcto:**

Ha relacionado correctamente cada uno de los conceptos con su respectiva respuesta. ¡Felicitaciones!, esto da cuenta de la comprensión de algunos conceptos claves del componente formativo. ¡Siga adelante con el mismo empeño!

**Incorrecto:**

Ha relacionado incorrectamente alguno de los conceptos con su respectiva respuesta, no se desanime, revise nuevamente el contenido del componente formativo y vuelva a intentarlo. ¡Mucho ánimo!