Primer examen de Seguridad II
Nombre:
Matricula:

1. Debes identificar el tipo de hash que utiliza el exámen (SI NO se incluye el procedimiento no se toma en cuenta.)(1%)
2. Comparar el hash con el que te proporciona el docente e identificar cual es el examen correcto. (SI NO se incluyen los procedimientos no se toma en cuenta.) (1%)

Para realizar el examen deberás ejecutar los siguientes pasos.
OJO se deberá entregar el archivo pcapng y en los puntos en que respondes debes pegar la trama de wireshark ó se anula la respuesta ya que para esta evaluación es indispensable demostrar la comprensión de este sniffer.

3. Deberás estar conectado a la red de la UAA.
4. Abre el wireshark e inicia una captura
5. Conectate al aula virtual
6. Consulta el material de la materia
7. Consulta tus tareas
8. Detén la captura de wireshark
9. Genera el archivo .pcapng y súbelo al espacio destinado para ese fin en aula virtual (1 %)
10. Copia y pega como texto las tramas en las que se efectúa el Three-Way Handshake entre tu máquina y el servidor del aula virtual. (2%)
11. Realiza la tabla con Mac O, Mac D, Ip O, Ip D, Puerto Origen, Puerto destino y aplicación del Three-Way Handshake. (5 %)
12. Indica la versión de TLS que utiliza el aula virtual. (1 %)
13. Sigue la secuencia de tramas en la que haces la consulta de lo solicitado en aulavirtual, indica que fue lo que te permite seguir la secuencia. y Desarrolla la tabla correspondiente (Mac O, Mac D, Ip O, Ip D, Puerto Origen, Puerto destino y aplicación) en la que demuestras el seguimiento encerrando con un círculo o con un color distinto lo que te permite seguir la secuencia (Al menos 6 tramas) (5%)
14. Identifica un conjunto de tramas donde se realice y resuelva una consulta DNS copialas y pegalas aquí identificando con estas tramas cual es el DNS de la UAA que te está resolviendo en primera instancia. (1%)
15. Realiza la tabla con Mac O, Mac D, Ip O, Ip D, Puerto Origen, Puerto destino y aplicación del DNS (5%)
16. Indica y demuestra que dominio está buscando y cual es la ip que corresponde al dominio buscado. (5 %)
17. identifica la Mac Address del router que está haciendo la función de gateway para ti.. Demuéstralo pegando una trama de wireshark (2%)
18. Desarrolla el esquema de ubicación (Gráfica, dibujo, plano) de dispositivos de cómputo en base a lo aprendido con la trama de wireshark capturada (4%).
19. Qué configuración necesitas realizar en un switch capa 3 cableado (“inteligente”) para poder usar un sniffer. (1%)

20. Toma alguna de las tramas usadas en los puntos anteriores que usen en su totalidad el protocolo TCP y alinea cada una de las partes de esta trama con el protocolo TCP/iP (2%)
21. Analiza la captura que se dejó en el espacio de examen llamada NTP_sync y especifica que es lo que se está haciendo y que equipos de cómputo participan.. Solo se toma en cuenta si se incluye la tabla (Mac O, Mac D, Ip O, Ip D, Puerto Origen, Puerto destino y aplicación) (2%)
22. Bajo qué controles de ISO 27001:2013 se justifica la implementación de un DRP y cada cuanto los colocarias tu para la UAA. (Justifica por qué) (1 %)
23. Basándonos en ISO 27001:2013 cada cuando realizamos los respaldos de la base de datos de alumnos de la UAA y como compruebas los respaldos. (1%)