Lo primero que tendría que hacer es instalar mi maquina virtual que nos dio con vmwarm y su sistema de kalipurple nos dio   
Curso de ciberseguridad:  
La ciberseguridad es la practica de proteger la infraestructura tecnológica, para poder implementar seguridad es implementar differentes procesos controles y herramientas.  
NIST Cyber security Framework

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identificar | Protección |  |  |  |

Blue team- equipos técnicas que establecen las medidas de seguridad para proteger la infraestructura  
red team: ciberseguridad ofensiva probar las implementaciones de blue team  
purple team asegurar que el blue team aprenad de las técnicas y tácticas utilizadas por rede team y mejore las medidas de seguridad

Triada cia (confidencialidad integridad disponibilidad) marco para guiar las políticas y practrivcas y controles de ciberseguridad que se establecen en un entorno tecnológico

Confidencialidad: capacidad de garantizar que la información no se encuentra disponible i es revelada a individuos que no tienen autorización para consultarla

Integridad: capacidad de garantizar la exactitud y completitud de la información a lo largo ed todo su ciclo de vida

Disponibilidad: capacidad de garantizar que la información se encuentra disponible siempre que se requiere

autenticación: proceso de verificar la identidad de un usuario

autorización: sigue a la autenticación, determinar que recursos ouede acceder y que acciones puede realizar.

no repudio: garantizar que cuando se realiza un intercambio de información el receptor de la información no puede negar haberla recibido, y el emisor de la información no puede negar haberla enviado.

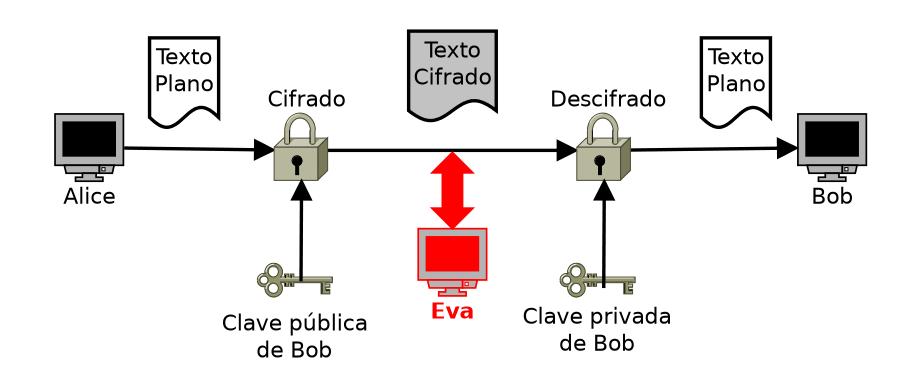
Amenaza ataque y vulnerabilidad   
amenaza: cualquier circunstancia o evento con el potencial de afectar negativamente

Vulnerabilidad: falla o debilidad en los procedimientos de seguridad de un sistema de información, diseño, implementación o controles internos que podría explotarse accidental o intencionadamente

Ataque: mecanismo a través del cual una amenaza explota una vulnerabilidad

Criptografía

Es la practica y el estudio de técnicas que permiten garantizar la confidencialidad integridad autenticación y no repudio de la información que se encuentra almacenada en el tránsito y el uso



Asunciones de seguridad

El cifrado de información no previenen la interceptación de la comunicación

El criptosistema no garantiza confidencialidad de extremo a extremo

El criptosistema suele ser publico

Kerckhoffs “la efectividad del sistema no debe depender de que su diseño permanezca en secreto”

Esto hace mención que entre mas personas lo vean se pueden sacar mas problemas y darle mas seguridad a tu sistema

Cifrado césar, cifrado de contenido militar  
este es un sistema de cifrado por sustitución en el que una letra en el texto original es reemplazado por la letra que se encuentra en un numero fijo en el abecedario

Decode.fr es una pagina para ver tipos de cifrados

Clasificación de los criptosistemas

La clave de cifrado/desifrado: simétricos y asimétricos o de clave publica

El tipo de txto plano que reciben: monoalfabeticos y polialfabeticos, numéricos

La manera en la que funcionan: transposición, sustitución, bloques, y stream

Las capacidades de seguridad que no proporcionan: confidencialidad, integridad, autenticación y no repudia

Ataques a un criptosistema (modelos)

Ciphertext-only attacks: el atacante conoce el algoritmo d ecifrado y algunos textos cifrados

Known-plaintext attacks: el atacante conoce el algoritmo de cifrado y algunso pares albitrarios de texto plano y cifrado

Chose-plaintext attacks: el atacante conoce el algoritmo de cifrado y algunos pares de texto plano y cifrado

Chose-cipher text ataca: el atacante conoce el algoritmo de cifrado y algunos pares de texto palnto y cifrado de los cuales a podido seleccionar el texto planto y o el texto cifrado

Rompiendo un criptosistema

Este esta se dice que está roto cuando existe un método para determinar el texto plano a partir del texto cifrado sin que involucre legítimamente la clave de descifrado.

Hay dos formas determinar la clave de descifrado y vulnerabilidad en el algoritmo de cifrado.

Metodos de ataque/fuerza bruta

Fuerza bruta es en Ciphertext-only attack

1. Intercepta el texto cifrado con un criptosistema conocido
2. Selecciona una clave del espacio de claves
3. Intenta desifrar el texto cifrado utilizando esa clave y comprobar si el resultado tiene sentido
4. Volver

Importancia del espacio de claves deben de existir suficientes claves de descifrado como para que no resulte práctico del proceso, todas las claves de cifrado deben tener la misma probabilidad de ser elegidas

Time memory trade off attacks:el tacante construye una tabla con textos cifrados a partir de textos planos que se envían con frecuencia utilizando un numero muy elevados de claves.

Cifrado simple por sostitucion

Corresponde con un tipo de cifrado en el que las letras del texto plano se sustituyen por otras letras del mismo alfabeto reordenado