4. Explicar la gravedad de este ataque en tres escenarios distintos cuando Alice inicia una comunicación con Bob.

- **Escenario 1: Alice y Bob realizan una compra online:**

El atacante (Eve) puede tener acceso a la información personal y financiera de Alice, como su nombre, dirección, número de tarjeta de crédito y código de seguridad, por lo que puede usar la información robada de Alice para hacer compras en su nombre.

- **Escenario 2: Alice y Bob se envían correos electrónicos confidenciales sobre datos de su empresa:**

El atacante (Eve) puede leer los correos electrónicos de Alice y Bob, que pueden contener información confidencial como contraseñas, secretos comerciales o datos personales y puede modificar y filtrar los correos electrónicos para crear confusión, sembrar discordia o manipular a Alice y Bob sobre su empresa.

- **Escenario 3: Alice y Bob se comunican a través de una red Wi-Fi pública:**

El atacante (Eve) puede interceptar las contraseñas de Alice y Bob cuando se conectan a la red Wi-Fi pública y puede acceder a los datos sensibles que Alice y Bob están transmitiendo a través de la red Wi-Fi pública, como información bancaria o médica.

5. Ver el Episodio 4 (Digits) de la Serie Connected de Netflix y discutir 2 aplicaciones potenciales de la ley de Bendfor a la criptología.

1. Para el análisis de claves criptográficas: La Ley de Benford puede usarse para analizar la distribución de los dígitos en claves criptográficas, como las utilizadas en el cifrado RSA, ya que en caso de que las claves no se generen de forma aleatoria y segura, es posible que la distribución de sus dígitos no se ajuste a la Ley de Benford, eso las haría vulnerable a ataques de fuerza bruta o análisis estadístico. En el episodio de Connected podemos ver cómo la Ley de Benford se puede utilizar para identificar claves RSA débiles, cuando los investigadores analizaron la distribución de los dígitos en las claves RSA publicadas por varios sitios web y encontraron que algunas de ellas no se ajustaban a la Ley de Benford. Lo que convierte a estos sitios web en sitios web vulnerables a ataques.

2. Detección de fraude en transacciones con criptomonedas: La Ley de Benford se puede usar para analizar la distribución de los montos de las transacciones en criptomonedas, esto se comprueba de manera que si las transacciones son legítimas, es probable que la distribución de los montos se ajuste a la Ley de Benford, pero si las transacciones son fraudulentas, es posible que la distribución de los montos no se ajuste a la Ley de Benford, lo cual nos da señales de que las transacciones son parte de un esquema de lavado de dinero u otra actividad ilegal. En el episodio de Connected, vemos cómo la Ley de Benford se puede utilizar para detectar fraude en transacciones con Bitcoin, cuando los investigadores analizaron la distribución de los montos de las transacciones en la red Bitcoin y encontraron que algunas de ellas no se ajustaban a la Ley de Benford.

6. Describir el modelo OSI.

El modelo OSI divide el sistema de comunicación de red en siete capas, que sirven para identificar los problemas de red.

El modelo Open Systems Interconnection (OSI) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar. En otras palabras, el OSI proporciona un estándar para que distintos sistemas de equipos puedan comunicarse entre sí. El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior.

Las capas son:

7. Capa de aplicación

6. Capa de presentación

5. Capa de sesión

La capa de sesión: sesión de comunicación

4. Capa de transporte

3. Capa de red

2. Capa de enlace de datos

1. Capa física

7. Mencionar cuáles son los ataques más conocidos a la capa 3 del modelo OSI.

1. Un ataque de denegación de servicio distribuido (DDoS) intenta sobrecargar a su objetivo con grandes cantidades de datos. Un ataque DDoS es como un atasco de tráfico que obstruye una autovía, impidiendo que el tráfico normal llegue a su destino.
2. En un ataque de Spoofing falsifican la dirección IP de origen de los paquetes para hacerse pasar por otro dispositivo.
3. En un ataque de fragmentación fragmentan paquetes TCP de forma maliciosa para evadir firewalls o sistemas de detección de intrusiones.

8. Sacar tus propias conclusiones sobre el protocolo Diffie-Hellman.

Me parece bueno en el sentido que permite a dos personas/usuario establecer una clave secreta compartida de forma segura, solo que es a través de un canal inseguro, además de que es usado en muchos protocolos criptográficos, como el protocolo TLS/SSL que protege las comunicaciones en internet y puede ser utilizado con diferentes algoritmos de cifrado y longitudes de clave. Sin embargo, considero que tiene un alto riesgo a ataques de

intermediario si no se implementa correctamente, ya que no autentica las identidades de las partes que participan en el intercambio de claves.

9. Subir el programa de Python al recopisotrio en GitHub. Y en PDF subir a la actividad el contenido adicional

LINK: https://github.com/KSofiaPerez14/SEGURIDAD_PEREZLOPEZ.git

Referencias:

- ¿Qué es el modelo OSI?| Ejemplos de modelos OSI | Cloudflare. (n.d.). Cloudflare. https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/