1.-Red Team Vs Blue Team

Red Team diseña ataques específicos para una red o sistema, explota sus vulnerabilidades, y tiene como objetivo reportar dichas vulnerabilidades al Blue Team. Blue Team evalua riesgos, diseña estrategias de mitigación y monitorea el sistema, su objetivo es proteger la infraestructura frente a los ataques detectados por el red team.

2.-CVE: Es una lista con las vulnerabilidades de seguridad conocidas, las cuales vienen con un resumen de las características, efectos, versiones del software afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.
Todas las CVE están clasificadas según CVSS también.

3.-CVSS: Es un modo de asignar un nivel de criticidad a una vulnerabilidad para evaluar su grado de gravedad de una forma estándar.

4.-PGP: (seguridad de mail) autenticidad, integridad y confidencialidad. Se usa a nivel mas personal. Sus operaciones contienen: firma digital, encriptación, criptografía de clave publica y privada, operaciones de compresión, compatibilidad de emails.

5.-S/MIME: (seguridad de mail) Se usa a nivel mas comercial. Sus operaciones incluyen la firma digital, encriptación, utiliza certificados de clave publica, sigue el modelo de pki hibrido.

6.-Estecanografia: Es ocultar información en cualquier archivo (imágenes, texto,…)

7.-PKI en Malla: admin

8.-Protocolo SET:
9.-Firma Dual del protocolo SET:

Ofrece privacidad al cliente y garantiza no repudio.

10.-Privacidad VS confidencialidad:

La privacidad está enfocada al derecho a proteger, controlar y decidir sobre el acceso y uso de información personal relacionada con la persona.
La confidencialidad sería la relacionada con los datos mientras la privacidad esta relacionada con la persona.

11.-Esquemas avanzados de la firma digital:

Firma ciega: permite que un firmante valide un mensaje sin conocer su contenido (como un voto electrónico).

Firma de grupo: cualquier miembro de un grupo puede firmar en nombre del grupo. Un administrador puede revelar al firmante en caso de disputas.

Firma de anillo: ofrece total anonimato, ya que un siquiera el administrador puede identificar al firmante.

12.-Enrrutamiento TOR VS ONION:

Los mensajes se cifran en múltiples capas, que se descifran progresivamente al pasar por cada nodo. (gofre y cebolla)

TOR sería un ejemplo avanzado:

ofrece anonimato mediante rutas aleatorias y cifrado

Imita ataques de correlación aplicando guardianes de entrada.

Foward secrecy, va cambiando de nodos cada 10 minutos.

Velocidad lenta y no garantiza privacidad de datos fuera de la red.

13.-TLS para qué, particularidad:

Es un protocolo criptográfico diseñado para proporcionar seguridad en las comunicaciones a través de redes informáticas, como internet. Evolución de SSL y utilizado para proteger datos durante la transmisión.
Propósitos: confidencialidad, integridad, autenticación y protección contra ataques intermediarios.
Se utiliza en: web, correo electrónico, VPNs , aplicaciones bancarias,…
Particularidades:
1.-Proceso de negociación(Handshake):

1.1.-Intercambio de parámetros (el cliente y servidor acuerdan los algoritmos de cifrado y autenticación que usaran.

1.2.-El servidor envia su certificado digital para demostrar su identidad.

2.-Intercambio de claves:

2.1.-Las partes generan una clave compartida(RSA, DHE/DH-Efimero)

3.-Verificacion:

3.1.-Verifican que las negociaciones fueron exitosas y la conexión segura se establece.

14.- IPSec para que, particularidad:

IPSec (Internet Protocol Security) es un conjunto de protocolos diseñado para proteger las comunicaciones en la **capa de red (capa 3)** del modelo OSI. Su objetivo principal es proporcionar **seguridad integral** a los datos que se transmiten a través de redes IP, tanto en IPv4 como en IPv6.

Propósitos principales de IPSec:

1. **Confidencialidad:** Cifra los datos para evitar que sean leídos por terceros.
2. **Integridad:** Asegura que los datos no sean alterados durante su transmisión.
3. **Autenticación:** Verifica que los datos provienen de una fuente legítima.
4. **Protección contra ataques de repetición:** Evita que un atacante capture y retransmita mensajes antiguos.
5. **Versatilidad:** Funciona tanto en redes privadas como públicas, y es especialmente útil para:
    - **VPNs (Virtual Private Networks):** IPSec garantiza que el tráfico entre dos redes o dispositivos sea seguro.
    - **Conexiones interempresariales:** Protege los datos en tránsito entre oficinas o sucursales.

Particularidades de IPSec

1. **Funciona en la capa de red:**
    - Opera a nivel de los paquetes IP, por lo que protege todo el tráfico que pasa por la red, sin importar el protocolo o la aplicación en las capas superiores.
    - Es **transparente para las aplicaciones**, lo que significa que no es necesario modificar las aplicaciones para usar IPSec.
2. **Modos de operación:**
    - **Modo Transporte:** Cifra solo la carga útil (payload) del paquete IP.
    - **Modo Túnel:** Cifra todo el paquete IP, incluyendo la cabecera original, y lo encapsula en un nuevo paquete IP.
3. **Protocolos asociados:**
    - **AH (Authentication Header):** Proporciona autenticación e integridad, pero no confidencialidad.
    - **ESP (Encapsulating Security Payload):** Proporciona cifrado, integridad y autenticación opcional.
4. **Gestión de claves:**
    - Utiliza **IKE (Internet Key Exchange)** para negociar las claves criptográficas y establecer asociaciones de seguridad (SAs).
    - Soporta múltiples algoritmos criptográficos como AES para cifrado y HMAC para integridad.
5. **Compatibilidad con IPv4 e IPv6:**
    - Aunque fue diseñado para IPv6, también funciona en IPv4, facilitando su uso en redes mixtas o en transición.
6. **Jerarquía de claves:**

    - IPSec utiliza un sistema jerárquico para manejar las claves de cifrado y autenticación, lo que mejora la seguridad y facilita la gestión.
7. **Flexibilidad en configuraciones:**
    - Puede proteger tanto comunicaciones punto a punto (entre dos dispositivos) como conexiones entre redes completas (mediante gateways o routers).

Ventajas de IPSec

1. **Protección integral:** Garantiza confidencialidad, integridad y autenticación para todo el tráfico de red.
2. **Transparencia:** No requiere cambios en las aplicaciones o protocolos de las capas superiores.
3. **Flexibilidad:** Soporta múltiples algoritmos de cifrado y modos de operación.
4. **Aplicaciones diversas:** Desde conexiones VPN hasta la protección de redes empresariales.

Limitaciones de IPSec

1. **Complejidad de configuración:** Requiere conocimientos avanzados para su correcta implementación.
2. **Sobrecarga de procesamiento:** Las operaciones de cifrado y autenticación consumen recursos significativos.
3. **No protege contra todo tipo de ataques:** Aunque protege los datos en tránsito, no impide ataques en las capas superiores, como el phishing o el malware.

Resumen: IPSec sirve para proteger el tráfico de red a nivel IP, ofreciendo confidencialidad, autenticación e integridad. Sus particularidades incluyen operar en la capa de red, su flexibilidad en modos de operación (transporte y túnel), y el uso de protocolos como AH y ESP. Es ampliamente utilizado en **VPNs** y redes empresariales para garantizar conexiones seguras.

15.-Diferencia entre firewall, IDS e IPS:

Firewall: filtra en base a reglas, y los deja pasar o no dependiendo de sus reglas.
IDS: Filtra en base a patrones según reglas, lanza alertas o las registra en un blog (no actúa).
IPS: hace lo mismo que IDS pero actúa, es decir puede bloquear paquetes que no cumplan sus requisitos.

16.-DMZ, objetivo:

Situados detrás del cortafuego, es una red aislada que da servicio al exterior y usualmente tiene un conjunto de reglas del cortafuegos más laxo.

17.-Protocolos que se usaban con IPSec:

IPSec utiliza dos protocolos principales para proporcionar **autenticación, integridad y cifrado** en las comunicaciones a nivel de red:

1. **AH (Authentication Header):**
   - Proporciona **autenticación** e **integridad** a los paquetes IP.
   - Asegura que los datos provienen de una fuente legítima y no han sido alterados.
   - **No cifra los datos**, solo los autentica.
   - Funciona encapsulando un encabezado adicional en el paquete IP original.
   - **Campos clave en AH:**
     - **Next Header:** Indica el tipo de protocolo que sigue.
     - **SPI (Security Parameter Index):** Identifica la asociación de seguridad.
     - **Sequence Number:** Evita ataques de repetición.
     - **Authentication Data:** Contiene un hash HMAC para verificar integridad y autenticación.
2. **ESP (Encapsulating Security Payload):**
   - Proporciona **cifrado**, además de **autenticación opcional**.
   - Protege tanto la **confidencialidad** como la **integridad** de los datos.
   - Funciona encapsulando la carga útil original del paquete dentro de un nuevo encabezado ESP.
   - **Campos clave en ESP:**
     - **SPI:** Identifica la asociación de seguridad.
     - **Sequence Number:** Protege contra ataques de repetición.
     - **Payload Data:** Datos cifrados.
     - **Authentication Data (opcional):** Para verificar integridad.

IKE (Internet Key Exchange):

- Aunque no es un protocolo que "transmite datos", es fundamental para IPSec porque gestiona las asociaciones de seguridad (SAs) y las claves criptográficas necesarias para AH y ESP.

18.-IPSec, modo de transporte VS túnel:

18. IPSec: Modo de Transporte vs. Modo de Túnel

IPSec tiene dos **modos de operación**, que definen cómo se aplican el cifrado y la autenticación al paquete IP:

Modo Transporte

- **Propósito:** Proteger solo los datos transportados (carga útil o payload).
- **Cómo funciona:**
  - Cifra y autentica únicamente la carga útil del paquete IP.
  - Las cabeceras IP originales permanecen intactas y visibles.
- **Uso típico:**
  - Comunicaciones punto a punto entre dispositivos finales, como servidores o estaciones de trabajo.
  - Ejemplo: Seguridad en una sesión de comunicación directa entre dos dispositivos.
- **Ventajas:**
  - Menor sobrecarga, ya que solo protege la carga útil.
  - Preserva la información original de la cabecera para su enrutamiento.
- **Limitaciones:**
  - No oculta las direcciones IP de origen y destino, por lo que es menos seguro frente a ataques de análisis de tráfico.

Modo Túnel

- **Propósito:** Proteger todo el paquete IP, incluyendo la cabecera.
- **Cómo funciona:**
  - Encapsula el paquete IP original completo (incluyendo su cabecera) dentro de un nuevo paquete IP con una cabecera diferente.
  - La cabecera externa contiene las direcciones IP del túnel (por ejemplo, de routers o gateways).
- **Uso típico:**
  - VPNs (Virtual Private Networks) para conectar redes completas a través de Internet.
  - Ejemplo: Conexión segura entre dos oficinas usando gateways IPSec.
- **Ventajas:**
  - Proporciona anonimato adicional al ocultar las direcciones IP originales.
  - Protege todo el paquete IP, incluyendo metadatos.
- **Limitaciones:**
  - Mayor sobrecarga debido al encapsulamiento completo del paquete.

Comparativa entre Modo Transporte y Modo Túnel

Aspecto	Modo Transporte	Modo Túnel
Qué protege	Solo la carga útil del paquete IP	Todo el paquete IP (cabecera + payload)
Cabecera IP visible	Sí	No (es encapsulada en una nueva cabecera)

Aspecto	Modo Transporte	Modo Túnel
Uso común	Comunicación entre dispositivos finales	Comunicación entre gateways (VPNs)
Sobrecarga	Baja	Mayor (encapsulamiento completo)
Anonimato	Bajo (cabeceras originales visibles)	Alto (cabeceras originales ocultas)

19.-Protocolos inalámbricos:

Introducción a la seguridad en redes inalámbricas

- **Particularidades de las redes inalámbricas**:
  - Comparten los mismos requisitos de seguridad que las redes cableadas (confidencialidad, integridad y autenticación).
  - **Amenazas adicionales específicas**:
    - El **medio de transmisión inalámbrico** aumenta los riesgos, ya que las señales pueden ser interceptadas o manipuladas sin acceso físico.
    - Los protocolos mal diseñados pueden introducir vulnerabilidades.
- **Puntos de ataque principales**:
  1. **Cliente o estación**: Dispositivos conectados a la red.
  2. **Punto de acceso (AP)**: El dispositivo que conecta la red inalámbrica a la red cableada.
  3. **Medio de transmisión**: La señal inalámbrica.
- **Amenazas comunes**:
  - **Robo de identidad MAC**: Suplantación de la dirección MAC.
  - **Ataques Man-in-the-Middle (MITM)**: Interceptación del tráfico entre cliente y servidor.
  - **Denegación de servicio (DoS)**: Sobrecarga que inhabilita el acceso.
  - **Inyección de mensajes**: Introducción de datos falsificados en la red.

---

2. Redes inalámbricas IEEE 802.11

El estándar **IEEE 802.11** define protocolos para redes inalámbricas y establece requisitos de seguridad para mitigar amenazas.

2.1 Diferencias clave entre redes cableadas y inalámbricas

- Las redes cableadas:
  - Ofrecen una autenticación implícita, ya que los dispositivos deben estar físicamente conectados.
  - Limitan el acceso físico al medio de transmisión.
- Las redes inalámbricas:
  - Requieren **mecanismos robustos de autenticación** y **cifrado**, ya que el medio es accesible para cualquier receptor cercano.
  - Las transmisiones pueden ser interceptadas fácilmente.

2.2 Protocolos de seguridad en redes inalámbricas

1. **WEP (Wired Equivalent Privacy):**
    - Diseñado para igualar la seguridad de las redes cableadas.
    - Basado en una clave compartida de 64 bits (40 bits para la clave secreta y 24 bits para el vector de inicialización).
    - **Vulnerabilidades:**
        - **IV débiles:** Reutilización de vectores de inicialización facilita la recuperación de la clave.
        - Uso del algoritmo RC4, que presenta problemas de seguridad en la implementación.
    - **Estado actual:** Obsoleto y no recomendado.
2. **WPA (Wi-Fi Protected Access):**
    - Introducido como una mejora intermedia del WEP dentro del estándar **IEEE 802.11i**.
    - **Características:**
        - Uso de **TKIP (Temporal Key Integrity Protocol)** con IVs más largos (48 bits).
        - Adopción del estándar **802.1X** para autenticación mediante **EAP (Extensible Authentication Protocol)**.
        - Mayor seguridad con soporte de AES (Advanced Encryption Standard).
    - **Limitaciones:**
        - TKIP heredó ciertas debilidades de RC4, por lo que también fue reemplazado.
3. **WPA2 (IEEE 802.11i):**
    - Introdujo el protocolo **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)** para reemplazar TKIP.
    - Uso exclusivo de **AES**, considerado más seguro.
    - **Servicios de seguridad principales**:
        - **Autenticación mutua:** Estación y servidor autenticador (como RADIUS) verifican sus identidades.
        - **Control de acceso basado en puertos:** Los clientes no tienen acceso a la red hasta que son autenticados.
        - **Integridad y confidencialidad:** Los datos se protegen mediante claves temporales y funciones de autenticación (HMAC).
4. **Fases de operación de WPA2:**
    1. **Descubrimiento:** El cliente identifica el AP más adecuado según su política de seguridad.
    2. **Autenticación:** Cliente y servidor autenticador se validan mutuamente.
    3. **Generación de claves:** Se establecen claves temporales para garantizar la confidencialidad.
    4. **Transferencia de datos protegida:** El cliente y el AP intercambian datos de forma cifrada.
    5. **Terminación de la conexión:** Finalización segura de la sesión.
5. **WPA3 (Revisión más reciente):**
    - Introduce **SAE (Simultaneous Authentication of Equals)** para mejorar la autenticación.
    - Cifrado de 192 bits en entornos empresariales.

    - Protección contra ataques de fuerza bruta offline mediante el uso de claves únicas por sesión.

---

3. Particularidades técnicas de WPA y WPA2

- **Jerarquía de claves:**
    - **PMK (Pairwise Master Key):** Generada durante la autenticación.
    - **PTK (Pairwise Transient Key):** Derivada de la PMK, se divide en:
        - **KCK (Key Confirmation Key):** Autenticación de mensajes.
        - **KEK (Key Encryption Key):** Cifrado de claves de gestión.
        - **TK (Temporal Key):** Cifrado de datos.
    - **GTK (Group Temporal Key):** Usada para transmitir datos grupales en redes compartidas.
- **Protocolos criptográficos:**
    - **TKIP:** Usado en WPA para compatibilidad con hardware antiguo.
    - **CCMP:** Introducido en WPA2, utiliza AES para cifrar datos.