Layer 2 Tunneling Protocol

* T2TP
* Comprende 2 protocolos: PPTP y L2FP
* Opera en la capa de enlace de datos
* Componentes: Acces Concentrator LAC y Network Server LNS
* Para la seguridad se combina con IPSec
* Comenzó en las redes telefónica

SSH

* Comunicación entre máquinas remotas
* Capa 7 modelo OSI
* Usa cifrado TLS
* Utilidades: Administración y acceso a recursos, Transferencia segura de archivos, creación de túneles de red.

WPA

* Wi-Fi Protected Access
* Sucesor de WEP
* Opera en la capa 2 de OSI
* Soporta 2 modos: Modo personal PSK y el modo empresarial WAP.
* Usa para encriptación el protocolo TKIT, AES, SAE.

PTPP

* Desarrollado por el Fórum PTPP
* Protocolos: LCP, GRE, PNS, ICMP, NCP, PPP, PAC, IGMP
* Mecanismos de autentificación: PAP, CHAP, MS-CHAP, MS-CHAP V2
* Proceso cifrado: conexión, autentificación, generación de clave, cifrado de datos, descifrado.

VPN

* Usos: Conexión anónima, acceso a servicios, seguridad y privacidad
* Protocolos más usados: PTPP, L2TP, SSTP, Open VPN, Ikev2
* Crea túnel seguro entre un dispositivo y el servidor remoto.

TLS

* Transport Layer Security
* Sucesor de SSL
* Capa 4 Transporte de OSI
* Componentes: Cifrado, Autentificación, Integridad
* Proceso: Negociación, Intercambio claves, Autentificación y establecimiento de sesión.

VLAN

* Divide una red física en subredes
* Tipos: datos, voz, administración, invitados
* Capa 2 y 3 OSI

Kerberos

* Usa sistema tickets
* Autentificación servidor cliente
* Ataques Man in the middle
* Opera en la capa 7 y 4 de OSI
* Componentes: Cliente, servidor, KDC que gestiona los AS y TGS.

WEP

* Capa 7 y 4 de OSI
* Componentes: Cliente web, Servidor web
* Protocolos: HTTP/HTTPS, DNS

IPSec

* Internet Protocol Security
* Capa 3
* Protocolos: AH, ESP, IKE
* Cifrado AES, 3DES, ChaCha20
* Autentificación HMAC

L2F

* Layer 2 Forwarding Protocol
* Desarrollado por cisco
* Capa 2
* Crea un túnel
* Roles LAC Y LNS

MIME

* Multipurpose Internet Mail Extensions
* Capa 7
* Cabeceras: Content type, Content transfer encoding

**1. Métodos de autenticación de usuarios**

1. **Autenticación basada en conocimiento**:
   * Uso de contraseñas o PINs. El usuario debe recordar y proporcionar un dato secreto.
2. **Autenticación basada en posesión**:
   * Utiliza dispositivos físicos como tarjetas inteligentes o tokens.
3. **Autenticación basada en características inherentes**:
   * Usa biometría como huellas dactilares, reconocimiento facial o de voz.
4. **Autenticación multifactor (MFA)**:
   * Combina dos o más métodos, como una contraseña y un código enviado al móvil.

**2. Métodos de control de acceso**

1. **Control de Acceso Discrecional (DAC)**:
   * Los propietarios de los recursos deciden quién puede acceder y qué permisos tienen.
2. **Control de Acceso Obligatorio (MAC)**:
   * Basado en etiquetas de seguridad asignadas al usuario y los datos. Es rígido y no permite cambios arbitrarios.
3. **Control de Acceso Basado en Roles (RBAC)**:
   * El acceso depende del rol asignado al usuario en el sistema.
4. **Control de Acceso Basado en Atributos (ABAC)**:
   * Permite acceso en función de atributos como ubicación, tiempo o tipo de dispositivo.

**3. Medidas de seguridad para bases de datos e inyección de código SQL**

1. **Medidas de seguridad**:
   * Uso de contraseñas fuertes y autenticación multifactor.
   * Cifrado de datos en tránsito y en reposo.
   * Uso de roles y permisos restringidos.
   * Auditorías regulares de bases de datos.
2. **Inyección SQL**:
   * Es un ataque donde el atacante inserta código SQL malicioso en una consulta legítima.
   * Ejemplo de ataque:

sql

Copiar código

SELECT \* FROM usuarios WHERE usuario = 'admin' OR '1'='1' AND contraseña = '';

* + Se realiza manipulando formularios o URLs mal diseñados.

**4. Tipos de software malicioso**

1. **Virus**:
   * Programas que se propagan al adjuntarse a otros archivos.
2. **Gusanos**:
   * Se replican y propagan automáticamente a través de redes.
3. **Troyanos**:
   * Aparecen como software legítimo, pero contienen funcionalidades maliciosas.
4. **Ransomware**:
   * Encripta datos y solicita un rescate.
5. **Spyware**:
   * Monitorea y recopila información del usuario sin su consentimiento.

**5. Ataques de denegación de servicio (DoS)**

* Consisten en saturar un sistema o red, dejándolos inutilizables para usuarios legítimos.
* **Tipos de ataques**:
  1. **Volumétricos**: Consumen ancho de banda.
  2. **Protocolos**: Explotan debilidades en el manejo de protocolos.
  3. **Aplicaciones**: Sobrecargan servicios específicos.

**6. Sistemas de detección de intrusos (IDS)**

* **Definición**:
  + Monitorean redes o sistemas para identificar actividades sospechosas.
* **Tipos**:
  + **Basados en firmas**: Detectan patrones específicos.
  + **Basados en anomalías**: Identifican comportamientos inusuales.

**7. Cortafuegos (Firewalls)**

* **Definición**:
  + Filtran tráfico entre redes para bloquear accesos no autorizados.
* **Defensa que provee**:
  + Controla conexiones entrantes y salientes.
* **Tipos**:
  + **De red**: Protegen redes completas.
  + **De host**: Protegen un dispositivo individual.
  + **De próxima generación (NGFW)**: Incluyen inspección avanzada y prevención de intrusos.

**8. Sistemas de prevención de intrusos (IPS)**

* **Definición**:
  + Bloquean ataques detectados en tiempo real.
* **Relación con IDS y honeypots**:
  + Los IPS actúan sobre las alertas generadas por IDS.
  + Los honeypots son sistemas señuelo diseñados para atraer atacantes.

**9. Desbordamiento de pila**

* Es un ataque que ocurre cuando se excede la capacidad de la pila en memoria, permitiendo la ejecución de código malicioso. Suele explotar funciones mal implementadas como gets().

**10. Recomendaciones para desarrollar software seguro**

1. Validar entradas y salidas.
2. Cifrar datos sensibles.
3. Implementar pruebas de seguridad.
4. Mantener bibliotecas y dependencias actualizadas.
5. Seguir estándares como OWASP.
6. Realizar auditorías y revisiones de código.