Protocolos de seguridad

OpenSSH

Conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, utilizando el protocolo SSH. Alternativa a Secure Shell, de software privado.

SCP (Secure CoPy)

Extensión de OpenSSH que permite copiar ficheros con seguridad entre dispositivos de red que tienen instalado un servidor SSH, que es otro de los componentes de SSH.

FTP

File Transfer Protocol, permite transferir archivos de un dispositivo a otro.

SFTP

SecureFTP, utiliza conexiones seguras utilizando SSH como túnel de seguridad.

SCP y SFTP

Herramientas cliente/servidor. Los clientes SCP y SFTP requieren que los servidores a los que se conectan provean los servicios homólogos.

IPSec

Internet Protocol Security, protocolo que define el cifrado, la autenticación y la gestión de claves para transmisiones TCP/IP.

Fases de IPSec

- ***Gestión de claves***: utiliza IKE como protocolo de gestión para el intercambio de claves entre origen y destino.
- ***Fase de cifrado***. En esta fase caben dos posibilidades. En el modo AH solo se cifra la cabecera del paquete. En el modo ESP se cifra el paquete completo.

- Los paquetes salen de PC1.
- Son asegurados en el dispositivo IPSec.
- Atraviesan internet hasta llegar al dispositivo IPSec de destino.
- Auténtica y descifra los paquetes para pasarlos a su destino final en el PC2.

S/MIME

Secure MIME, protocolo de alto nivel usado para hacer seguro el envío de mensajes y transacciones electrónicas incluyendo cifrado y firma digital mediante criptografía RSA.
Secure / Multipurpose Internet Mail Extensions es un estándar de clave pública utilizado en correos electrónicos. S / MIME compite con técnicas equivalentes como PGP y PEM.

Monitorización del tráfico de red

Un sniffer o monitor de red es un software que monitoriza continuamente el tráfico de red de una estación o servidor conectado a la red con la posibilidad de capturar todo el tráfico y creando un histórico de la actividad.
Los sniffers suelen:

- Monitorizar el tráfico en un segmento.
- Capturar el tráfico generado en el segmento.
- Capturar las tramas enviadas hacia o desde un nodo específico.

Algunos monitores especializados en redes inalámbricas podrán:

- Identificar las estaciones inalámbricas y puntos de acceso.
- Miden la potencia de la señal y determinar el rango de los puntos de acceso.

Seguridad en las redes inalámbricas

Protocolo WEP

Wire Equivalent Privacy, primer protocolo que quiso que el medio inalámbrico tuviera una seguridad similar al cableado. Utiliza claves para autenticar a los clientes y para cifrar sus conexiones. La clave de cifrado es conocida por los clientes y el propio punto de acceso. La clave sirve de cifrado como también de autenticación.
Utiliza claves de 64, 128, 256 bits, fácil de romper. Envía IV en texto plano, haciéndolo más vulnerable.

Protocolo IEEE 802.11i y 802.11n

802.11i identifica dispositivos y proporciona dinámicamente a cada transmisión su propia clave. Utiliza un TKIP como sistema de gestión y generación de claves de cifrado. Requiere un autenticado recíproco entre el punto de acceso y el cliente.
Puede utilizar AES como método de cifrado. IEEE 802.11n integra a 802.11i . Reconocido internacionalmente como el estándar para comunicaciones Wifi.

WPA y WPA2

WPA es un subconjunto del estándar 802.11i aprobado por la Wi-Fi Alliance que surge como una alternativa más segura que WEP. No es tan seguro como 802.11i.
Tanto WPA como 802.11i siguen el mismo mecanismo, se diferencia en que WPA cifra con RC4 y 802.11i con AES.
WPA2 sustituye a WPA integrando cifrado AES. Teóricamente WPA2 es invulnerable.

Seguridad perimetral

Son sistemas que están en contacto tanto con la LAN interna como con internet o una red externa. Los equipos están especialmente sobreexpuestos por lo que se requerirá una especial atención.

Concepto de IDS (Sistema de Detección de Intrusos)

Detecta manipulaciones no deseadas en los sistemas o ataques no detectados por los cortafuegos mediante análisis de tráfico de red. Basado en la monitorización de eventos y la gestión posterior de alertas basadas en reglas. Existen 3 tipos básicos de IDS:

- ***HIDS (Host IDS)***: sistema que vigila un único sistema.
- ***NIDS (Network IDS)***: sistema que se basa en la red.
- ***DIDS (Distributed IDs)***: sistema basado en la arquitectura cliente-servidor que está compuesto por múltiples NIDS, actuando como sensores centralizando la información.

DMZ

Red desmilitarizada o DMZ, zona de la red segura que se encuentra entre la red local y la red externa. Se ubican los servidores que tengan que ser accesibles desde la red externa. El cortafuegos o un router de borde restringe el acceso desde el exterior de la DMZ, permitiendo únicamente el acceso a algunos puertos de algunos sistemas.

Ataques Internos y Externos

El principal riesgo será el atacante que penetre en el sistema. Una vez ahí, se hace más compleja la arquitectura del ataque.

Puntos destacables en la red interna

- Antimalware y cortafuegos.
- Realizar un enfoque multicapa.
- Tener actualizados los sistemas.
- Dispones de un IDS eficaz.

Punto destacable de la red perimetral

- Es la parte que sufre la máxima exposición al ataque.
- Los principales problemas se centran en los puertos TCP o UDP.
- La seguridad es inútil si se descuida la seguridad en la red interna.
- Los ataques con éxito a la red perimetral deterioran la credibilidad y el prestigio de la organización.

Herramientas para la seguridad perimetral

- Traducción de direcciones IP o puertos.
- Protocolos de túnel.
- Bloqueo de puertos de comunicación.