TEMA 8. SEGURIDAD EN LAS COMUNICACIONES

Contenido

NIVELES OSI

- NIVEL FISICO:
    - Funciones:
        - Activar y desactivar conexiones
        - Switch, cables, …ETC
    - El objetivo en cuanto a la seguridad:
        - Garantizan cableados
        - Dispositivos tengan medidas de protección
    - Medidas de seguridad a adoptar.
        - Controles biométricos
        - Empleo de SAI

- NIVEL ENLACE:
    - Hace referencia a la trasferencia de datos entre diferentes nodos de la red
    - En esta capa se encuentra:
        - MAC
        - Definiciones VLAN
        - Protocolos para las WANS
    - Vulnerabilidades:
        - Falsificar las direcciones MAC
        - Localizar redes inalámbricas mediante programas
    - Medidas a tomar:
        - Filtrado MAC
        - Cifrado clave de conexiones inalámbricas

- NIVEL DE RED:
    - Se define el diseño de la red lógica.
    - La función es que la información llegue al receptor.
    - Dispositivo principal es el Router.
    - Se trabaja con IP
    - Vulnerabilidades:
        - Suplantación IP (modificando la cabecera del paquete de información)
        - **Ataques DoS** (degeneración de servicio) se genera tráfico excesivo mediante técnicas de Spoofing.
    - Medidas:
        - Sistema de detección de intrusos
        - Firewall
        - Limitar Ips
        - Filtros de correos

- NIVEL TRANSPORTE (Información llegue a su destino)
    - Debe controlar los puertos mediante Netstat.
    - Controlar el tráfico a través de los puertos.

- NIVEL DE SESIÓN

  Este nivel se encarga de la relación entre usuarios y la red.

    - Vulnerabilidad: es la acción de los sniffer
    - La medida de seguridad es la utilización del Firewall.

Ejemplos de amenazas(explicados en amenazas y ataques en el tema 7)

1- **DoS o denegación de servicio**: Provoca que un servicio no sea accesible a los usuarios no pudiendose conectar debido a una sobrecarga de los recursos, mediante bonet (ordenador contaminado) o red zombie se pueden llegar a controlar cientos de miles de máquinas.
2- **Sniffing:** Consiste en monitorizar el tráfico de una red.
3- **Man in the Middle (MiM**): Un atacante supervisa una comunicación entre dos partes falsificando las identidades de los extremos y recibir el tráfico en los dos sentidos.
4- **Spoofin**g: Suplantación de identidad. Falsificar IP, MAC, WEB…

REDES CABLEADAS

– GENERALIDADES

- Una máquina que ofrece servicios TCP/IP debe abrir puertos.
- Las primeras redes LAN cableadas eran muy inseguras, porque todos los ordenadores estaban conectados al mismo cable (estructura en bus).
- Actualmente la arquitectura en estrella tiene un cable directo al Switch (envía paquetes). El Switch decide el puerto para enviar los paquetes
- Vulnerabilidades de redes conmutadas:
  - **Protegen Switch físicamente** (armario/rack)
  - **Protegen Switch lógicamente** (poner usuario y contraseña)
  - Hay que **hacer grupos de puertos** porque en un switch suelen estar conectados grupos de máquinas que nunca necesitan comunicarse entre ellas.
  - **Controlar que equipos se pueden conectar y a que puertos**

– VLAN

- **VLAN**: Grupos de puertos que se hacen en un Switch gestionables para aislar un conjunto de maquinas
- Aparenta estar en una LAN propia
- Mejora rendimiento y seguridad porque las maquinas solo hablan entre ellas
- Una VLAN basada en grupo de puertos no queda limitada a un Switch, algún puerto puede ser parte de otro grupo.
- Es raro que VLAN esté aislada, ya que necesitan conexión a Internet y conectarse con otros servidores externos.

– AUTENTICACION EN EL PUERTO MAC Y 802.1x

- **Dirección MAC**→Dirección del nivel 2 en una tarjeta, se asigna por el fabricante, por lo que una tarjeta no puede ser igual que otra.
- **Para evitar los ataques**, los Switch deben permitir establecer y autenticar en los puertos solo aquellas MAC que estén en la lista del propio Switch, dado que esto se puede falsificar se puede utilizar un software mediante un servidor Radius.

SEGURIDAD EN LA CONEXIÓN A REDES LOCALES NO FIABLES

- La conexión a Internet nos permite intercambio de información, y cuando navegamos estamos enviando la dirección ip de nuestra máquina.
- Si alguien se hace con ella podríamos ser víctimas de un ataque.
- Existen herramientas que permiten proteger los equipos de la red, como son los cortafuegos y los proxys

PRACTICA 1 DE SPYWARE

PROTOCOLOS SEGUROS

– SSL

- Proporciona seguridad en las comunicaciones por una red (Internet)
- Proporciona autenticación y privacidad entre extremos, mediante el uso de criptografía.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

– TLS

- Es una evolución del SSL
- Permite establecer una conexión segura mediante un canal cifrado entre cliente y servidor

– FTP SEGURO

- Soportan conexiones seguras y cifradas sobre SSH y SSL y TLS

– IPSEC

- Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo IP, cifrando cada paquete IP
- Actúa sobre la capa 3

– HTTPS

- Protocolo seguro de transferencia de hipertexto
- Se emplea para conexión a páginas web, que hay que proteger los datos que se intercambian con los servidores.
- Utiliza cifrado SSL y TLS
- Trabaja sobre el puerto 443
- Está basado en el intercambio de claves y uso de certificados válidos.
- La confianza que proporciona HTTPS se basa en una autoridad certificadora.
- Lo soporta la mayoría de los navegadores
- Es habitual en las webs en tiendas en línea, bancos…

– SSH

- Permite acceder a equipos remotos a través de la red de forma segura
- Trabaja de forma similar a TELNET
- Incorpora técnicas de cifrado que protege la información que viaja por la red, de modo que un Sniffer no pueda hacerse con el usuario y su contraseña usados en la conexión, ni conseguir los datos que se intercambian.
- Cualquier equipo puede configurarse como un servidor SSH en cualquier sistema operativo

EJERCICIO 2 DE PRÁCTICAS

SEGURIDAD EN LAS REDES CABLEADAS

– 1. VPN

- Redes privadas virtuales
- Permiten mediante internet establecer una conexión realizando una inversión económica moderada
- Para tener seguridad en esa conexión y comunicación es necesario:
  - **Autenticación y autorización**
  - **Integridad**→ ver que la información que hemos enviado no se ha cambiado
  - **Confidencialidad**→se hacen algoritmos de cifrado
  - **No repudio**→ los mensajes tienen que estar firmados

– ARQUITECTURAS DE VPN

- **VPN acceso remoto**→ modelo más usado y tanto los usuarios como los proveedores que se conectan a la empresa pueden hacerlo desde cualquier sitio mediante internet
- **VPN punto a punto**→ son conexiones remotas con oficinas o con una sede central, el servidor VPN está conectado permanentemente a internet y para la comunicación utiliza la técnica del tunneling (se encapsula un protocolo de red sobre otro creando un túnel dentro de la red)
- **VPN over LAN**→arquitectura menos difundida. Emplea la misma red de LAN de la empresa aislando zonas y servicios a los que se le añaden cifrados. En el uso de túneles cifrados se utilizan sobre todo los protocolos IPSEC o SSL

¿Qué es una VPN?

Una VPN o Red privada virtual es, básicamente, una red virtual que se crea dentro de otra red, habitualmente Internet.

Para un cliente VPN se trata de una conexión que se establece entre su equipo y el servidor de su organización, esta conexión es transparente al usuario.

El objetivo final de la VPN es que el usuario (empleado de la empresa) **no note si está en la empresa o fuera de ella.** En ambos casos recibe una configuración IP privada.

El responsable de conseguir esta transparencia es el software de la VPN.

- En el ordenador del empleado hay que instalar un software cliente VPN.
- Este software instala un driver de red, de manera que para el sistema operativo es una tarjeta más.
- Ese driver se encarga de contactar con una máquina de la empresa, donde ejecuta un software servidor VPN que gestiona la conexión para introducir los paquetes en la LAN. La gestión consiste en:
  - **Autentificar al cliente** VPN. Usuario/contraseña.
  - **Establecer un túnel a través de internet**. El driver de la VPN en el cliente le ofrece una dirección privada de la LAN de la empresa, pero cualquier paquete que intente salir por esa tarjeta es encapsulado dentro de otro paquete. Este segundo paquete viaja por Internet desde la IP pública del empleado hasta la IP pública del servidor VPN en la empresa. Una vez allí, se extrae el paquete y se inyecta en la LAN.
  - **Proteger el túnel**. Los paquetes encapsulados irán cifrados.
  - **Liberar el túnel**. El cliente o servidor puede interrumpir la conexión cuando lo consideren necesario.

Instalación y configuración de una VPN

Cuando implementemos una VPN, será necesario realizar la instalación y configuración de dos partes bien diferenciadas, el servidor y el cliente.

Los sistemas Windows, incorporan una utilidad para establecer redes privadas virtuales de un modo sencillo y guiado, mediante la configuración de una conexión de red avanzada.

También existen muchas aplicaciones software que nos permiten crear VPN, las cuales ofrecen diferentes niveles de seguridad y posibilidades distintas para la configuración

http://goo.gl/yCpsh ==> como crear una VPN en Windows

EJERCICIO 3 DE PRÁCTICAS

2. DETECCION DE INTRUSOS

- Herramientas de seguridad que detecta y monitoriza eventos
- Busca patrones definidos de actividades sospechosas
- Aportan prevención ya que alertan de forma anticipada
- No detienen ataques solo previenen
- Tipos
  - HIDS→protegen un servidor (pc o host)
  - NIDS→protege un sistema basado en red, actúa sobre la red capturando y analizando paquetes.
- En cuanto a la ubicación se recomienda ponerlo uno delante y otro detrás de un cortafuegos en una red perimetral.
- En general, lo que hace es:
  - Detección de ataques y barridos de puertos, que permiten alertar sobre cualquier anomalía o ataque.

– 3. ARRANQUE DE SERVICIOS

- Un servicio de un sistema operativo es una aplicación que corre en segundo plano
- Se pueden instalar varios servicios, pero ralentiza el sistema operativo.
- Para evitar que se ejecuten automáticamente servicios no deseados, los sistemas incorporan el control de cuentas de usuario, para evitar que ciertos usuarios ejecuten programas dañinos.

EJERCICIO 4 DE PRÁCTICAS

– 4. SERVICIOS DE RED

- NMAP y NETSTAT
- Las herramientas NMAP están disponibles para Windows y para Linux, se encargan de escanear puertos para ver los servicios disponibles; esta herramienta puede intentar la conexión a cada uno de ellos, analiza mensajes
- La información que nos ofrece es útil, ya que entre otras nos muestra la versión de los sistemas y las aplicaciones, por lo que un atacante podría detectar de forma rápida las vulnerabilidades

Para cada puerto la herramienta ofrece cuatro posibles estados:

- Open: (abierto) la máquina acepta paquetes dirigidos a ese puerto, donde algún servidor está escuchando y los procesará adecuadamente.
- Closed (cerrado). No hay ningun servidor escuchando.
- Filtered Nmap no puede decir si ese puerto está abierto o cerrado porque alguien está bloqueando el intento de conexión (router, firewall)
- Unfiltered el puerto no está bloqueado, pero no se puede concluir si está abierto o cerrado.

SEGURIDAD EN REDES INALAMBRICAS

Lo más habitual en redes Wi-fi es **la topología infraestructura** en la que existe un **punto de acceso que hace de switch**, de manera que los demás ordenadores se conectan a él, le envían sus paquetes y él decide cómo hacerlos llegar al destino. El punto de acceso es el encargado de gestionar el proceso de comunicación entre todas las estaciones Wifi.

- **Ventajas:**
  - Movilidad→Conexión desde cualquier punto
  - Escalabilidad→añade equipos sin coste alguno
  - Flexibilidad→Conectividad en cualquier momento y lugar.
  - La instalación de la tecnología inalámbrica -> es simple y económica

- **Inconvenientes:**
    - **Menor rendimiento**: el ancho de banda es mucho menor.
    - **Seguridad**: cualquiera que esté en el alcance de la red puede aprovechar una vulnerabilidad para colarse en la red o descifrar los mensajes. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad.
    - **Interferencias**: la red es mucho más sensible a interferencias.

Para tratar estas cuestiones de seguridad se han desarrollado técnicas para ayudar a proteger las transmisiones inalámbricas, por ejemplo, la encriptación y la autenticación.

La **autenticación es más habitual en redes inalámbricas** que en redes cableadas. Los AP admiten varios tipos de autenticación:

- **Abierta**: no hay autenticación, cualquier equipo puede asociarse con el AP.
- **Compartida**: la misma clave que utilizamos para cifrar la usamos para autenticar.
- **Acceso seguro**: usamos distintas claves para autenticar y cifrar. El usuario solo necesita saber una, la clave de autenticación: la clave de cifrado se genera automaticamente durante la asociación.
- **Autenticación por MAC**: el AP mantiene una lista de MAC autorizadas y solo ellas pueden asociarse.

Recomendaciones de seguridad en WLAN

Una red wireless es por definición **más difícil de proteger** que una red convencional entre otras cosas porque el medio es el aire y así como en una LAN tenemos una toma de red determinadas y controladas, en principio, en una WLAN se puede acceder desde cualquier punto que permita la antena.

Medidas básicas pero efectivas no en el 100% de los casos pero se impide el acceso a la gran mayoría de los intrusos.

- Colocación de la Antena: El primer paso para cerrar el acceso no autorizado a nuestro punto de acceso es colocar la antena de este de manera que limite el alcance de la antena a nuestra área de trabajo. Nunca hay que colocar una antena cerca de una ventana ya que el cristal no bloquea la señal. Un

esquema ideal seria colocar la antena en el centro del área dejando que solo una leve señal escape a través de los muros o ventanas de la oficina o lugar de trabajo.

- Cambiar la contraseña por defecto.
- Aumentar la seguridad de los datos transmitidos. Usar encriptación WEP o WPA/WPA2 o servidor Radius.
- Ocultar tu red Wi-fi. Cambiar el SSID por defecto

  El Service Set Identifier (SSID) es la cadena de identificación usada por los clientes de un AP para ser capaces de iniciar una conexión. Este identificador viene predefinido por el fabricante y cada uno viene con una cadena por defecto, por ejemplo los 3Com vienen con "101".
  Los intrusos que conozcan estas cadenas por defecto pueden acceder con relativa facilidad a una WLAN y hacer un uso de ella, generalmente no muy bueno...
  Desactivar el broadcasting SSID, o identificador de la red inalámbrica
  El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente el nombre y los datos de la red inalámbrica, evitando así la tarea de configuración manual.

  Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

- Evitar que se conecten. Activa el filtrado de direcciones MAC. Establecer el número máximo de dispositivos que puedan conectarse. Deshabilitar el servicio DHCP.
- Para los más cautelosos: Desconecta el AP cuando no lo uses. Cambia las claves regularmente.

EJERCICIO 5 Y 6 DE PRÁCTICAS