TEMA 6 SEGURIDAD ACTIVA EN REDES

1. SEGURIDAD EN LA CONEXIÓN A REDES NO FIABLES

Mecanismos de defensa perimetrales – defensa de ataques externos

Mecanismos de defensa internos – defensa de ataques internos

Cada vez que nos conectamos a Internet se produce un intercambio de información entre nuestro equipo y la red. Este intercambio es necesario para que podamos acceder a la información y servicios de Internet, pero si no tenemos garantías de seguridad es necesario limitar la información que es enviada, ya que en otro caso podría ser utilizada sin nuestro consentimiento.

Existen diversas herramientas que nos permiten proteger los equipos de la red, como los **cortafuegos** y los servidores **proxy**, que veremos en los temas 7 y 8 y otras técnicas que abordaremos en este tema.

Mecanismos de defensa perimetrales - defensa de ataques externos:

Router
Subredes
Cifrado de las comunicaciones
Sistemas de detección de intrusos (IDS)
Firewall perimetral
Proxy
Conexiones VPN
DMZ
Ofrecer el mínimo número de servicios
…

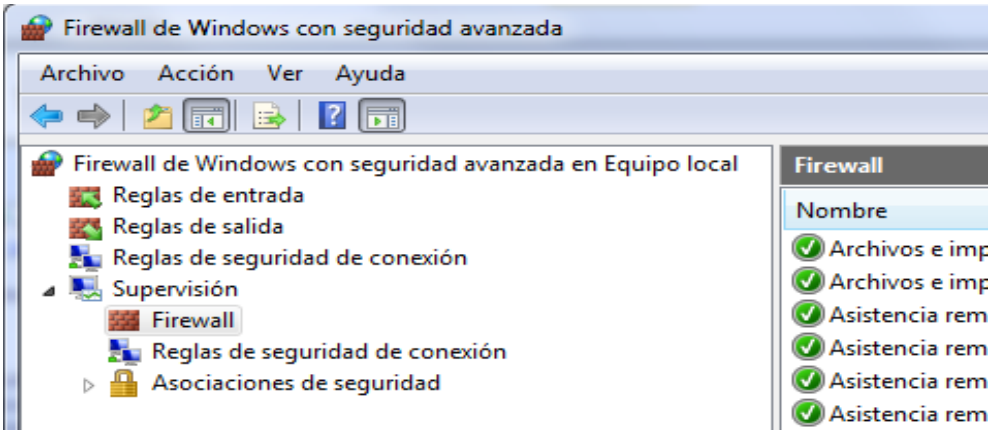
Mecanismos de defensa internos - defensa de ataques internos:

Listas de control de acceso (ACL)
Conexiones SSH
Auditorias de seguridad
VLAN
Contraseñas
Anti-malware
Programación segura
Detección de intrusiones
Controlar y minimizar los recursos compartidos
Controlar la instalación de software
Actualizar el software
…

1.1 CORTAFUEGOS LOCAL

Cortafuegos

Protegemos nuestro equipo controlando el tráfico que atraviesa la tarjeta de red de nuestro equipo tanto en el sentido de salida como en el sentido de entrada a nuestro equipo.



Ejercicio: Activar y configurar un **cortafuegos local**:

Cortafuegos local de Windows XP
Cortafuegos local de Windows 7
Cortafuegos local de Windows 2012 Server
Cortafuegos local de Ubuntu Desktop

Nota: Habilitar el protocolo ICMPv4 en el cortafuegos local de un equipo W7

- Ir a Inicio, Panel de control, asegúrate que del lado superior derecho este seleccionado ver por iconos grandes o icono pequeños, luego busca y abre el icono Firewall de Windows.
- Del lado izquierdo elige la opción configuración avanzada, aguarda a que se abra la ventana de Configuración avanzada y selecciona Reglas de entrada, haz clic con el botón derecho sobre Reglas de entrada y selecciona la opción Nueva Regla.
- Selecciona regla personalizada y presiona siguiente. Selecciona todos los programas y luego presiona siguiente.
- En tipo de protocolo debes seleccionar ICMPv4, presiona siguiente.
- Deja las dos configuraciones en Cualquier dirección IP y presiona siguiente.
- Selecciona permitir la conexión y presiona siguiente.
- Deja las tres opciones marcadas y presiona siguiente.
- Elige un nombre a la nueva regla por ejemplo PING y presiona finalizar.

1.2 SPYWARE / ANTISPYWARE

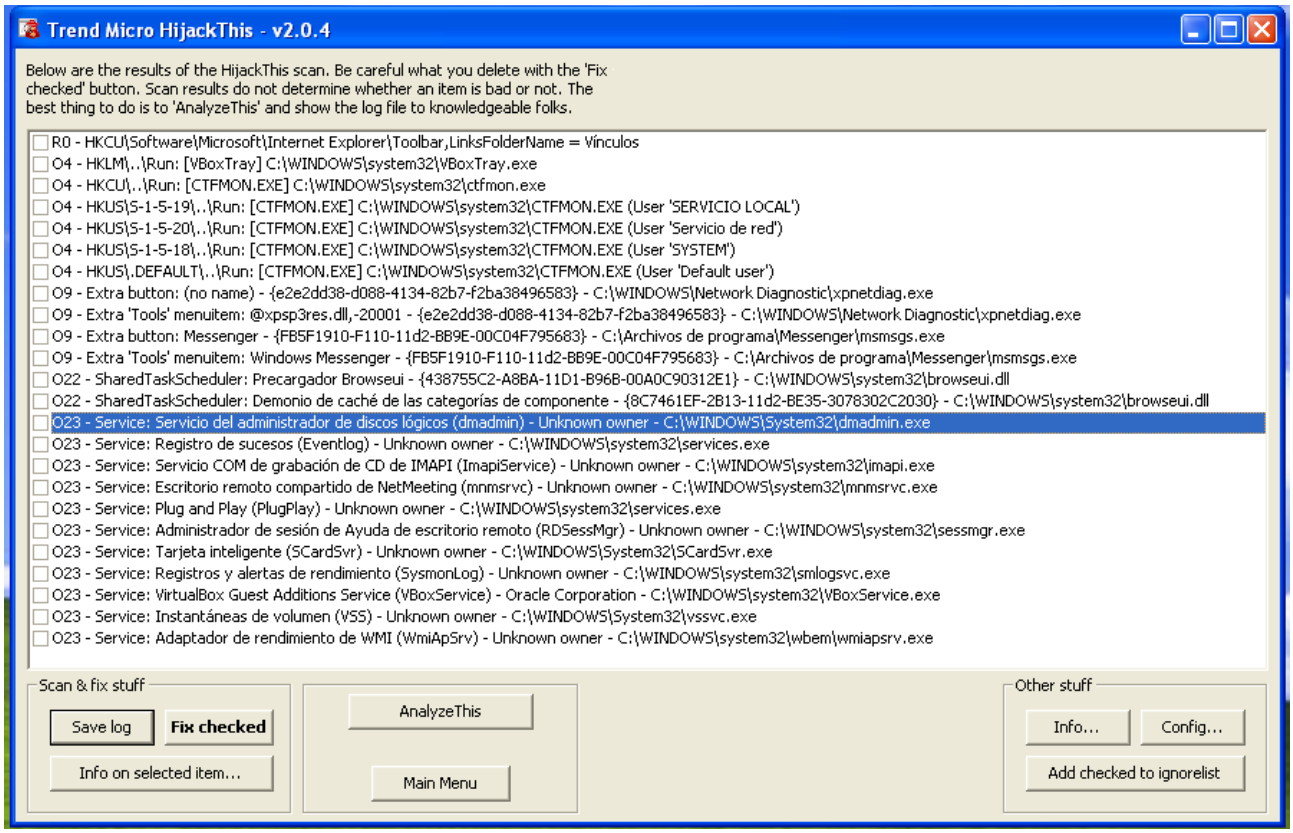
HijackThis ***Spyware***

Navegar por Internet, recibir correos con archivos adjuntos o incluso instalar algún programa con licencia Freeware sin leer sus condiciones de uso pueden traer un invitado inesperado a nuestro equipo, un spyware.

Un **Spyware** es, en definitiva, un pequeño programa que se instala en nuestro equipo con el objetivo de espiar nuestros movimientos por la red y de robar nuestros datos, de modo que a través de él puede obtenerse información como nuestro correo electrónico y contraseña, la dirección IP de nuestro equipo, nuestro teléfono, páginas buscadas y visitadas, así como cuanto tiempo se pasa en ellas, descargas realizadas, compras con la tarjeta, número de la tarjeta, etc. A medida que recopilan esta información la envían a empresas de publicidad en Internet para comercializar con nuestros datos.

Ejercicio: **Detección de Spyware/Malware y Virus con HijackThis**

HijackThis es una herramienta gratuita para Windows que nos permite detectar y eliminar intrusos en nuestro equipo.



1.3 ANTIVIRUS

Antivirus

Programas cuyo objetivo es detectar y/o eliminar virus informáticos.

Ejercicio: **localiza información en Internet sobre la historia del desarrollo de los virus informáticos.**

1.4 HTTPS

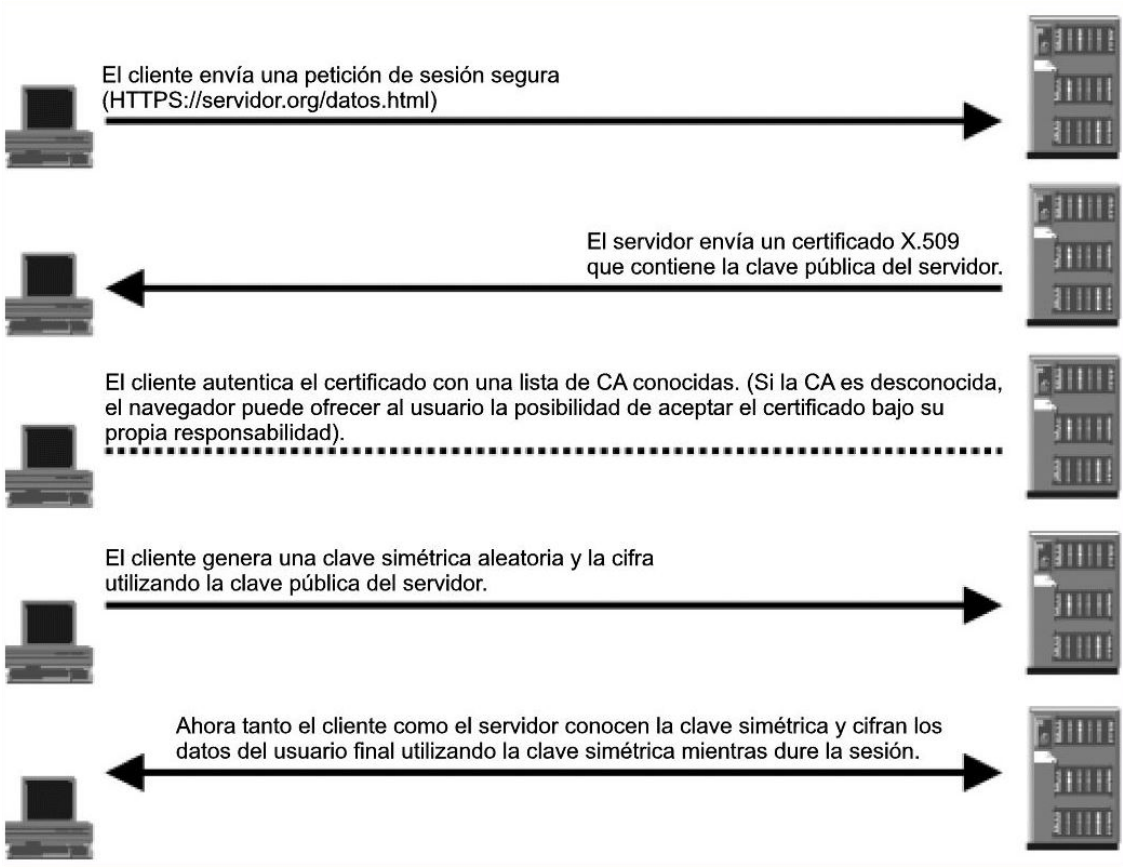
HTTPS

El protocolo **HTTPS** es la alternativa segura al uso de HTTP. Sus siglas corresponden a ***Hypertext Transfer Protocol Secure*** y se emplea para conexiones a páginas web en las que hay que proteger los datos que se intercambian con los servidores.

El objetivo de HTTPS es proporcionar una conexión segura sobre un canal inseguro. Se basa en el intercambio de claves y el uso de certificados válidos, verificados por una autoridad de certificación que garantiza que el titular del mismo es quien dice ser, de modo que un atacante no pueda hacerse pasar por dicho servidor.

HTTP trabaja por defecto con el puerto TCP 80 y HTTPS con el puerto **TCP 443**.

Establecimiento de conexión HTTPS:



Ejercicios: **Instalación y configuración de servicios y clientes HTTPS**

Conectarse a un servidor web seguro y analizar el certificado que utiliza.
Montar un servidor HTTPS sobre Windows 2012 Server
Montar un servidor HTTPS sobre Ubuntu Server

1.5 CONEXIÓN REMOTA SEGURA – SSH

SSH

El protocolo ***Secure Shell*** (Interprete de ordenes seguro, **SSH**) nos permite acceder a equipos remotos a través de una red y copiar datos que residen en ellos de forma segura, utilizándose como alternativa al uso de Telnet.

Cualquier equipo puede configurarse como un **servidor SSH**, instalando una pequeña aplicación y configurándola adecuadamente.

Para acceder a este equipo debemos instalar un **cliente SSH** en el equipo desde el que pretendemos comunicarnos (y tener conectividad con el servidor SSH).

OpenSSH es la versión del protocolo ssh mas utilizada.

Las claves privada y pública del servidor generadas con ***ssh-keygen*** se guardan en los ficheros:

/etc/ssh/ssh_host_key
/etc/ssh/ssh_host_key.pub

En el caso de los clientes los nombres de los ficheros y su ubicación cambian, pero se suelen guardar en el directorio raíz de cada cuenta, dentro del directorio ***.ssh***, con los nombres ***identity*** y ***identity.pub***.

El servidor se llama ***sshd*** y los clientes pueden ser ***ssh***, ***sftp***, ***slogin***, ***scp***, … además de otros programas que funcionan con entorno gráfico como ***Notepad++***,***Putty***,...

El fichero de configuración del servidor sshd está en ***/etc/ssh/sshd_config*** donde podemos configurar:

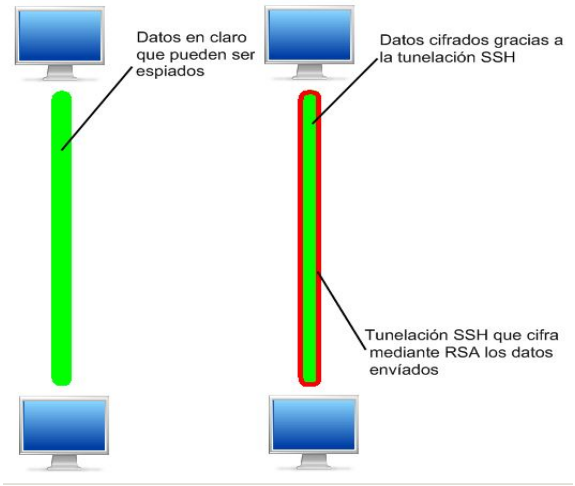
Direcciones IP de los clientes
Puerto TCP del servidor (22 por defecto)
Fichero que contiene la clave privada
Longitud de la clave
Permitir acceso desde la cuenta root (recomendamos ponerlo a no)
Permitir el acceso a cuentas sin contraseña (recomendamos ponerlo a no)
StrictMode: Comprobación de los permisos de acceso al directorio raíz antes de establecer la conexión (lo correcto es no desactivar esta opción)
RSAAuthentication y *PasswordAuthentication*: métodos de autenticación autorizados.

La configuración de los clientes también podemos consultarla en el fichero ***/etc/ssh/ssh_config***.

Ejercicio: Instalación y configuración de servicios y clientes SSH

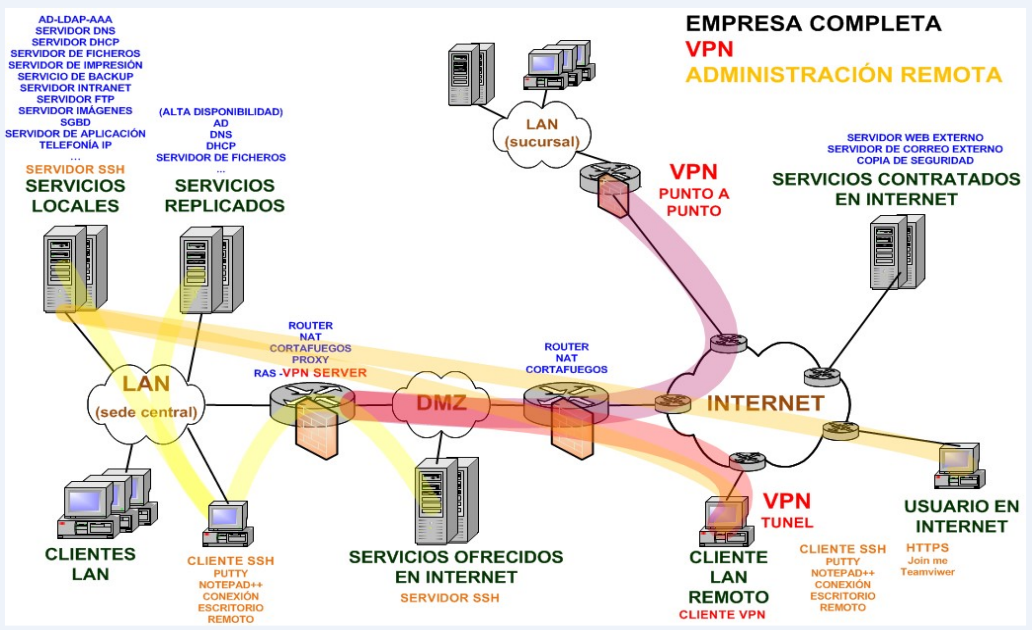
Configura un servidor SSH sobre Ubuntu Server.
Configura un servidor SSH sobre Windows 2012 Server.
Configura un servidor SSH sobre XP.
Configura un cliente SSH para realizar una conexión remota a las máquinas anteriores.

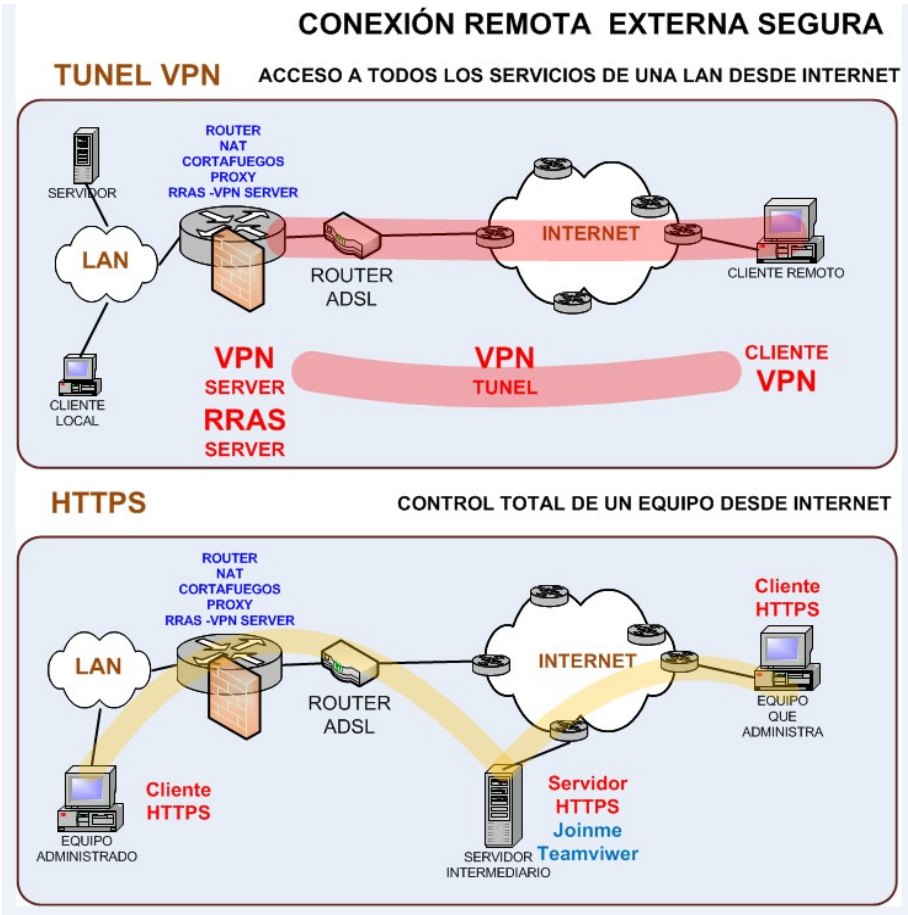

Identificación SSH mediante clave
Enviar clave SSH pública
Las claves públicas coinciden
Inicio de la sesión SSH
Id_rsa
Id_rsa.pub
authorized-keys
El cliente SSH almacena las claves pública y privada
En el servidor SSH hay un archivo que contiene las claves públicas autorizadas


Datos en claro que pueden ser espiados
Datos cifrados gracias a la tunelación SSH
Tunelación SSH que cifra mediante RSA los datos envíados

1.5.1 ADMINISTRACIÓN Y CONTROL REMOTOS

La administración de los servidores de nuestra empresa la realizaremos de forma segura y remota: desde otro equipo de la LAN (normalmente) o desde un equipo en Internet.





Administración remota de Windows (desde la LAN)

CONEXIÓN A ESCRITORIO REMOTO

Configuración en el servidor: habilitar la conexión a escritorio remoto

Configuración en el servidor: habilitar las cuentas o grupos que van a utilizar la conexión a escritorio remoto.

Configuración en el cliente Windows: ejecutar el cliente de conexión a escritorio remoto.

CONEXIÓN REMOTA SSH SOBRE EQUIPOS WINDOWS

Configuración del servidor ssh sobre Windows.

Configuración del cliente ssh: Putty,…

Administración remota de linux (desde la LAN)

OPENSSH

La suite OpenSSH incluye:

ssh, reemplaza a rlogin y telnet para permitir shell el acceso remoto a otra máquina. ssh tero@ejemplo.com

scp, reemplaza a rcp scp tero@ejemplo.com:~/archivo .

sftp, reemplaza a ftp para copiar archivos entre dos computadoras sftp tero@ejemplo.com

sshd, el servidor demonio SSH sshd

ssh-keygen, una herramienta para inspeccionar y generar claves RSA y DSA que son usadas para la autenticación del cliente o usuario.

ssh-agent y **ssh-add**, herramientas para autenticarse de manera más fácil, manteniendo las claves listas para no tener que volver a introducir la frase de acceso cada vez que utilice la clave.

ssh-keyscan, que escanea una lista de clientes y recolecta sus claves públicas.

El servidor OpenSSH puede autenticar a los usuarios mediante todos los métodos estándar del protocolo ssh

Conexión remota SSH sobre equipos Linux

Instalación del servicio ssh.

Configuración del servicio ssh

Configuración del cliente **Putty**

Configuración del cliente **Notepad++**

Utilizado para documentar ficheros de configuración.

Utilizado para modificar ficheros de configuración desde un entorno gráfico (para ello la cuenta de conexión debe tener permisos de escritura sobre el fichero… lo que nos lleva a tener que habilitar el password del root o a modificar los permisos del fichero de configuración para la cuenta que estamos utilizando).

Conexión SSH con acceso al entorno gráfico Linux

ssh -X

Gestión de certificados en SSH

Generar nuestro propio certificado

Utilizar nuestro propio certificado en la conexión ssh.

Administración remota basada en HTTPS (desde Internet)

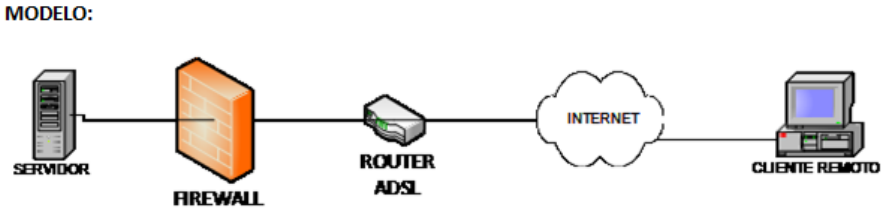
Join me

Teamviwer

NOTA: este método de administración remota se salta todos los cortafuegos, no es necesario tener abierto ningún puerto de entrada en la empresa.

Administración remota a través de VPN (desde Internet)

Modelo:



Planteamiento:

Elegir los sistemas operativos de las máquinas (Servidor, Firewall y cliente)
Implementar el firewall
Probar la no conectividad internet-servidor.
Generar los certificados necesarios.
Implementar un servidor ssh sobre el servidor con los certificados generados.
Implementar una VPN entre el cliente y el firewall.
Probar la conectividad segura cliente remoto –servidor.

Implemetaciones posibles – Planteamiento teórico

TELNET

Terminal Services (Terminal Server)

http://technet.microsoft.com/es-es/library/cc546615%28en-us%29.aspx
http://www.microsoft.com/spain/windowsserver2008/virtualization/terminal.mspx

SSH

OpenSSH

PuTTY

Acceso remoto SSH Secure Shell con PuTTy
http://www.aemilius.net/soporte/manuales/acceso-ssh-ssl-secure-shell-telnet-PuTTY.html

Radmin

http://www.radmin.es/products/radmin/
http://www.radmin.es/products/radmin/security.php

HTTPS

Join me

Teamviwer
Logmein

VNC

http://www.realvnc.com/

CLIENTES QUE FACILITAN LA EDICIÓN Y EL SERVICIO FTP

NOTEPAD++

http://notepad-plus-plus.org/

WINSCP

http://winscp.net/eng/docs/lang:es

VPN

Ejercicio obligatorio:

Administración remota del servidor Windows desde la LAN basada en la **conexión a escritorio remoto**.

Administración remota del servidor Linux desde la LAN basada en **Putty** y **Notepad++**

(Para Notepad++) Gestión de las cuentas de usuario que tienen permiso de modificación sobre los ficheros de la máquina remota.

Estudio del formato de intercambio Windows / Linux para que los ficheros creados con Notepad++ de almacenen correctamente en la máquina Linux.

Administración remota de un equipo desde Internet utilizando **join.me**

Administración remota de un equipo desde Internet utilizando **TeamViwer**

Instalación de TeamViwer como servicio (en Widows): **TeamViwer Host** (punto 12.2. del manual)

Ejercicio avanzado:

Implementación de una VPN para un puesto de trabajo desde casa conectado a la LAN de la empresa

Gestión de certificados y utilización en la conexión remota segura.

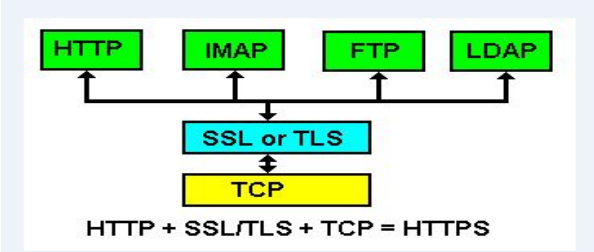
Conexión remota entre la sede central de una empresa y sus dos sucursales basada en VPN punto a punto.

1.6 SSL/TLS

SSL/TLS

Protocolo seguro que trabaja entre la capa de aplicación y la capa de transporte para hacer seguros a los protocolos de la capa de aplicación que utilizan TCP a través de él:

identificador	puerto TCP	descripción
https	443	HTTP sobre SSL
smtps	465	SMTP sobre SSL
nttps	563	NTTP sobre SSL
ldaps	646	LDAP sobre SSL
telnets	992	TELNET sobre SSL
imaps	993	IMAP sobre SSL
ircs	994	IRC sobre SSL
pop3s	995	POP3 sobre SSL
ftps-data	989	FTP-Datos sobre SSL
ftps-control	990	FTP-Control sobre SSL



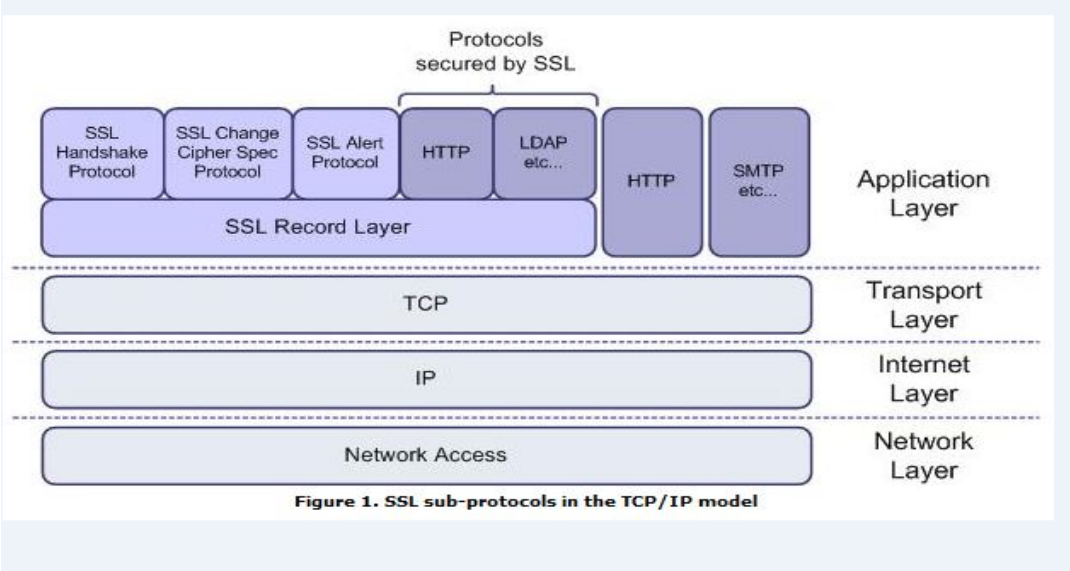
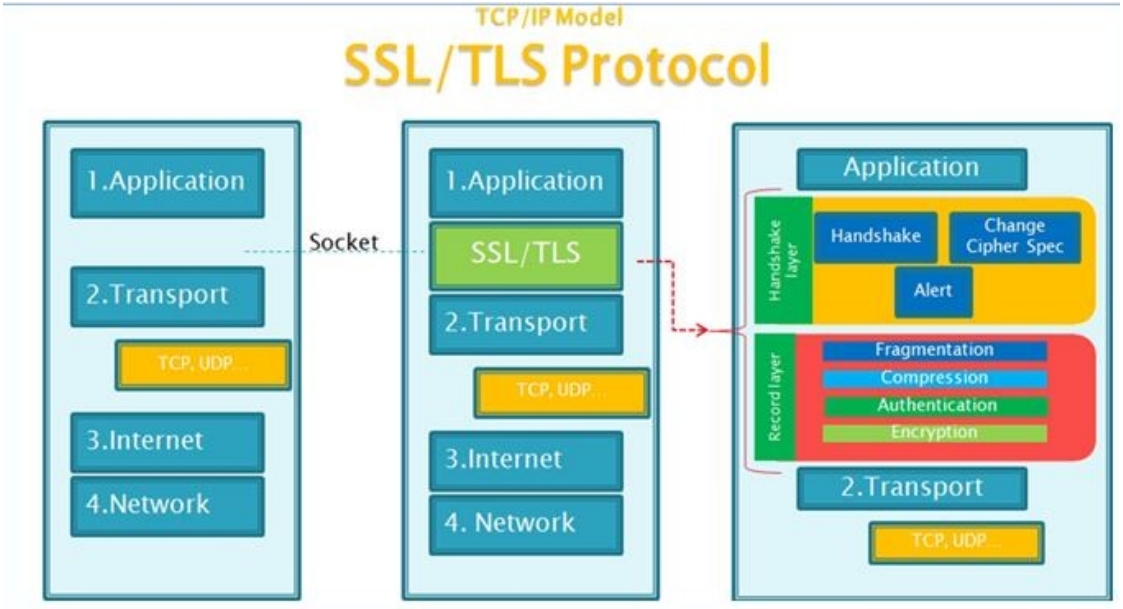


Figure 1. SSL sub-protocols in the TCP/IP model



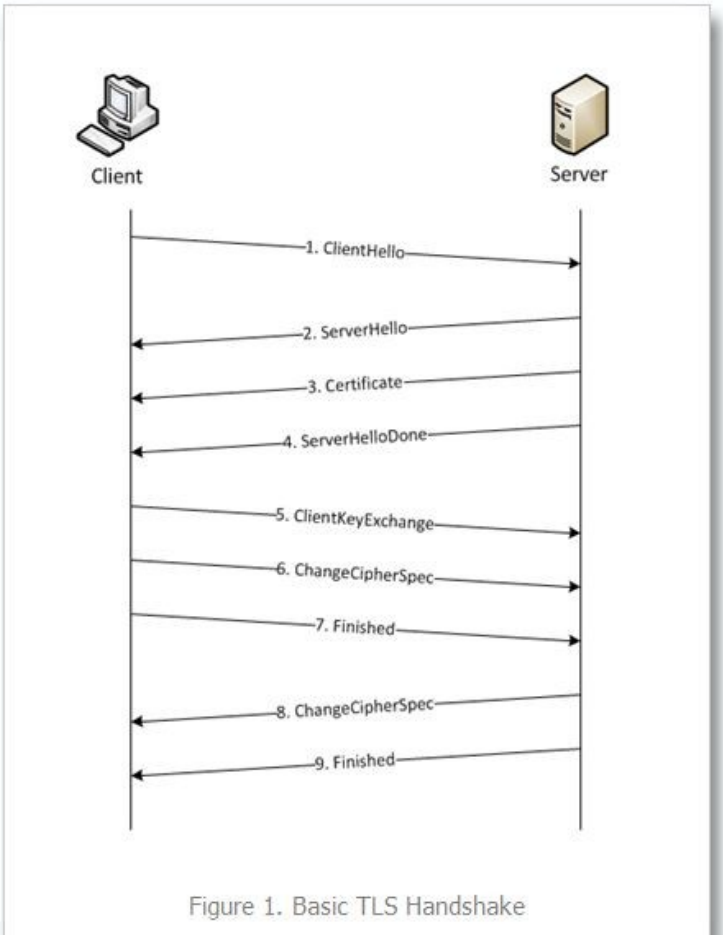


Figure 1. Basic TLS Handshake

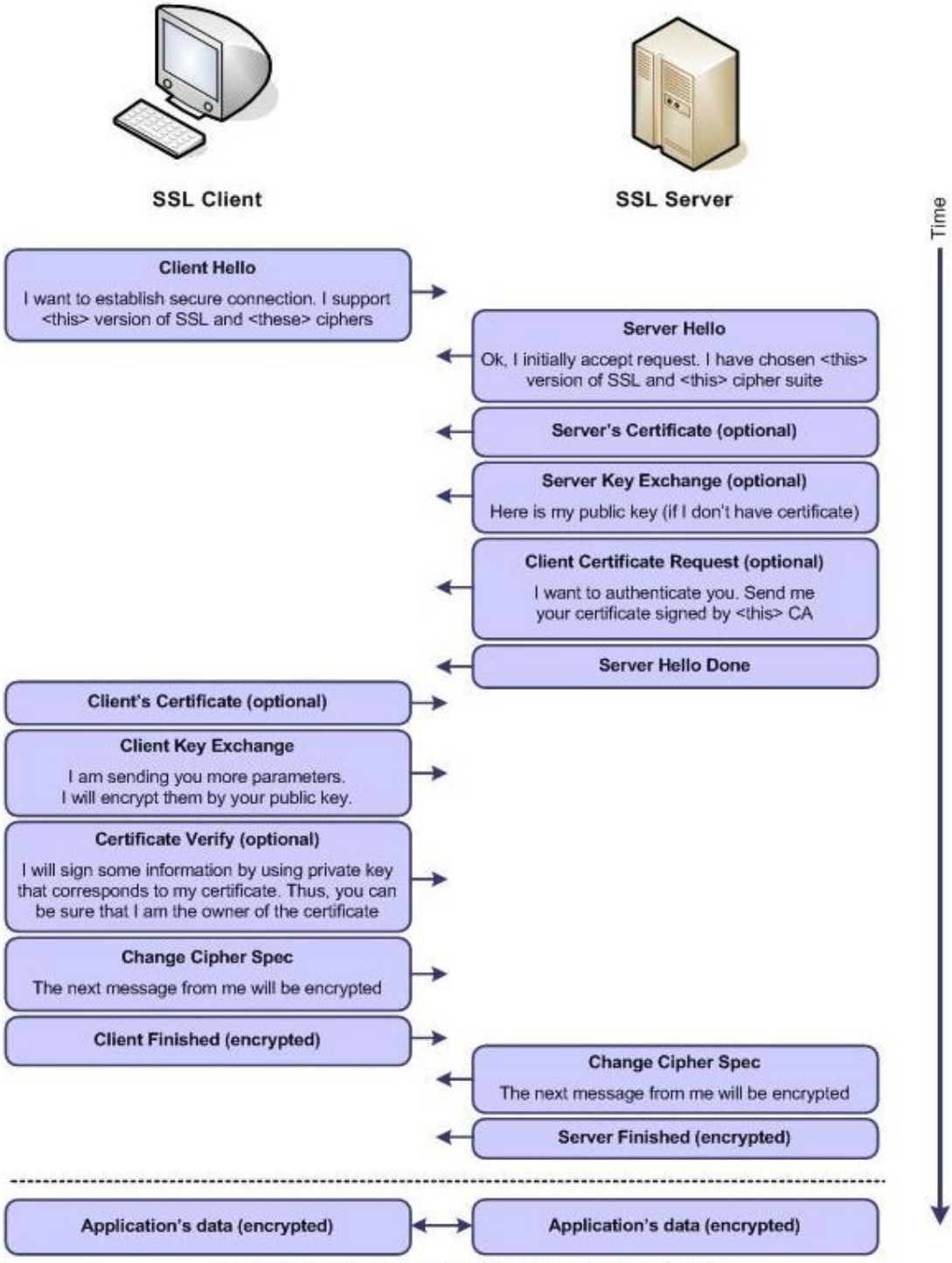


Figure 2. How SSL established connections, step-by-step.

1.7 OTROS PROTOCOLOS DE SEGURIDAD

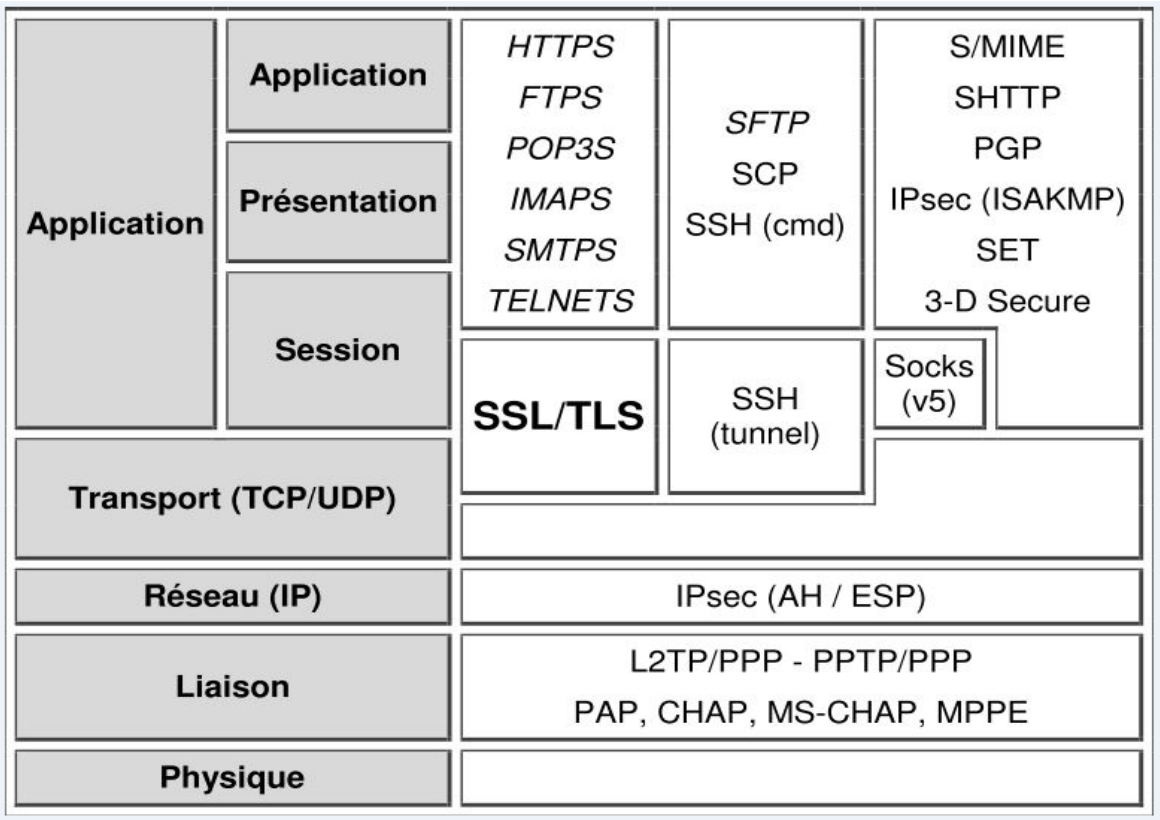
IPSec ***IPv6*** ***WPA – 802.11*** ***VLAN – 802.1Q***

L2TP ***AAA Server***

RADIUS

Microsoft RAS – Servidor de Acceso Remoto: Introducción y configuración

Utilización de líneas de comunicaciones dedicadas



2. SEGURIDAD EN REDES CABLEADAS

Medio de transmisión ***Simulador de red*** ***Modelo de red***

Software de monitorización de red ***Sistema detector de intrusos (IDS)***

2.1 ADMINISTRACIÓN, DISEÑO Y DOCUMENTACIÓN DE RED

Disponer de un modelo de red actualizado es básico para poder mejorar y proteger los sistemas de comunicaciones y los propios sistemas

Programa de modelado de red

Medios de transmisión

Velocidad de transmisión: Es el tiempo que se tarda en enviar un paquete (desde el primer bit al último), se mide por bits por segundo.

Ancho de banda: Es la cantidad de datos que se puede enviar por unidad de tiempo. Se mide en bits por segundo (bps)

Normas y estándares: Cableado estructurado – Elementos y espacios de una red.

- **ISO/IEC 11801**: Especifica el cable para telecomunicaciones en edificios (LAN) o grupos de ellos (CAN).
- **ISO/IEC 14763**: Mantenimiento y documentación del cableado de un edificio.
- **IEC 61935**: Especificaciones de prueba de cableado.
- **EN 50175**: Normativa para la instalación de sistemas de cableado estructurado en la Unión Europea.
- **EN 50174**: Instalación de cable de telecomunicaciones en edificios.
- **EN 50289**: Comprobación de los cables de comunicación.

Simuladores de red: Programas que permiten dibujar, modelar y/o simular redes.

Visio
Packet Tracer de CISCO
Kiva

Monitorizadores, Escaneadores o Mapeadores (Network Management Software): software de monitorización que escanea la red creando mapas de las redes. Ideales para monitorizar y administrar redes que ya están creadas.

LANsurveyor
WhatsUpGold

Certificación del cableado: las pruebas del cableado pueden hacerse:

Simples

TIA-568-B cuando existen problemas
TIA-568-B para certificación
ISO 11801:2002 para certificación

La **certificación** es una forma de demostrar que se han cumplido todas las normas y estándares. La certificación de un proyecto debe contener los siguientes elementos:

- Planos: de situación, trazados y enumeración de todas las tomas.
- Memoria descriptiva del proyecto que debe incluir la relación del material, incluyendo marcas, modelos, características técnicas,… Incluir la documentación de los fabricantes en los anexos.
- Memoria de las pruebas realizadas de todos los segmentos, rosetas, enlace permanente,… Para cada toma se realizarán unas pruebas que se documentarán en fichas con :
  - ✔ Identificación del enlace
  - ✔ Ubicación del enlace
  - ✔ Fecha de la realización
  - ✔ Operador
  - ✔ Identificación de equipos de pruebas, versión del software del tipo de prueba
  - ✔ Especificación del cable usado
  - ✔ Resumen general del test (PASS/FAIL)
  - ✔ Mapa de conexión de los hilos de esa toma
  - ✔ Resistencia e impedancia de cada par de hilos
  - ✔ Tiempo de propagación por los pares y diferencia de retardo de la señal.
  - ✔ Longitud
  - ✔ Prueba de perdida de retorno (RL), diafonía (NEXT), relación atenuación/diafonía (ACR) y ELFEXT, locales y remotas
- Memoria de pruebas de fibra óptica

Ejercicio: busca videos en YouTube sobre como se ha cableado el fondo marino desde Europa a Estados Unidos (buques cableros, cable de fibra óptica marina, cableado marino).

Testeo de cableado

Linkware: Programa de testeo de cable de flukenetworks

Recomendaciones en la instalación de cableado

- Usar siempre rosetas y conectores de la misma categoría que el cable
- Evitar que el cableado pase por varios cuartos de distribución. Que pase por el mínimo.
- Asegurarnos de que sea improbable la entrada de agua por el cable.
- No tender el cable tensado.
- Cumplir con las recomendaciones de curvatura de los estándares.
- Alejarnos de los tendidos eléctricos. Se recomienda alejar los cables lógicos (datos) de los eléctricos.
- Contar con un enchufe eléctrico por cada puesto de trabajo o tres por cada 10m2.
- Se respetará la topología en estrella. Nada de Hubs y menos en cascada.
- Utilización de cables antiincendio o que no imitan gases tóxicos en su combustión y que tengan protección antirroedores.
- Diseñar la arquitectura de cableado en AutoCAD u otra aplicación de Diseño.

Etiquetado de cables

La norma EIA/TIA-606 especifica que cada terminación de hardware debe ser etiquetada de modo que lo identifique de forma exclusiva, esto incluye los dos extremos de cualquier cable.

Utilización de códigos de colores.

Montaje de armarios

http://www.gonzalonazareno.org/praredes/p11c/p11c.html
https://www.youtube.com/watch?v=kM6IiGuEZFY

Protocolos de red

Protocolo de comunicaciones ***Protocolos de red***

Es un conjunto de reglas que permite a dos máquinas comunicarse entre sí en una red aunque tengan una arquitectura y sistemas operativos diferentes.

Los protocolos de red pueden estar implementados con software, hardware, firmware, o bien una mezcla de ellos.

Los protocolos deben ser los mismos en ambas máquinas para que se pueda establecer la comunicación.

2.2 MONITORIZACIÓN DE RED – LOG DE SERVICIOS – IDS

Sistema detector de intrusos (IDS)

Software de monitorización

Las herramientas de software de monitorización de la red buscan defectos o tráficos lentos, remitiendo resúmenes y estadísticas.

Los programas más recomendados para la monitorización de red son: Cisco LMS, Colasoft, Intermapper, LogicMonitor, Microsoft Network Monitoring, **Munin**, **Nagios**, Nimsoft UM, Orion NP, **PRTG NM**, Snort, Splink, Wireshark y Zenoss.

- Permiten trending o estadísticas y tendencias.
- Permiten IP SLA. Porcentaje de disponibilidad de IP.
- Casi todos permiten análisis de equipos a posteriori o en caliente.
- Algunos permiten la posibilidad de tener agentes o software cliente que remite datos de apoyo a la monitorización.
- Soportan el protocolo SMTP.
- Soportan la grabación del syslog: registro de datos del tráfico.
- Incluyen alertas ante determinados problemas.
- Administración y/o monitorización vía web.
- Soportan IPV4 e IPV6.
- Supervisión distribuida.
- Base de datos accesible SQL.
- Permiten crear mapas de redes.
- Control de acceso restringido para la administración.

Sistemas de detección de intrusos (IDS)

Programa utilizado para detectar accesos no autorizados a un computador (**HIDS**) o a una red (**NIDS**).

Ejemplo de HIDS: **Tripwire**

Ejemplo de NIDS: **Snort**

2.3 ESCANEO DE RED: IP, PUEROS, DNS, SERVICIOS, RECURSOS COMPARTIDOS,...

Sniffer *Wireshark* *Nmap* *Nessus* *WifiSlax*

Ping

Traceroute

Analizador de tráfico (**Sniffer**) de red	**wireshark**
Software para redes wi-fi	**wifislax**
Rastreador de puertos:	**nmap**
Escaneo de vulnerabilidades:	**nessus**
Kali linux	**Kali linux (wikipedia)**

Ejercicio: **Realiza un reconocimiento de red desde tu ordenador**

Utilizar **nmap** para realizar un barrido ping o un rastreo sigiloso del espacio de dirección que utilizamos.
Tenga en cuenta si los sistemas se encuentran protegidos por un muro de fuego o no.

Utilizar **nessus** para realizar rastreos de vulnerabilidades de los equipos identificados.
Antes de realizar este ejercicio, hablar con el administrador de red (profesor) para no provocar ningún incidente de seguridad.

3. SEGURIDAD EN REDES WIFI

Roaming – itinerancia ***WDS*** ***Portal cautivo***

En los últimos años, las necesidades de comunicación en empresas y en los hogares han cambiado mucho, y no solo en la velocidad de las conexiones a Internet. El uso de ordenadores portátiles y otros dispositivos móviles: teléfonos móviles, consolas portables, PDA… se ha disparado.

Este tipo de equipamiento exige conexiones inalámbricas que permitan la movilidad.

Existen varios tipos de conexiones inalámbricas: Bluetooth, Wi-Fi, 3G, ... Nos centraremos en Wi-fi por ser las que proporcionan acceso a una red de área local.

Ventajas de las redes inalámbricas:

Movilidad: nos permite conectarnos desde cualquier punto (dentro del alcance de la red inalámbrica).
Escalabilidad: podemos añadir equipos fácilmente y con un coste reducido.
Flexibilidad: permite colocar un equipo en cualquier punto (no es necesaria una toma de red).

Inconvenientes de las redes inalámbricas:

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.
Interferencias: la red es mucho mas sensible a interferencias.

3.1 802.11

El estándar **802.11** define los primeros niveles de la capa OSI para las redes de área local inalámbricas WLAN.

Protocolos estándar que permiten la comunicación inalámbrica:

802.11a
802.11b
802.11g
802.11n

Los dispositivos electrónicos que interactúan entre si pueden seguir diferentes estándares y tendrán que ser compatibles entre ellos para poder comunicarse.

Conceptos en redes Wi-fi:

- Conexión ad-hoc
- Conexión puente
- Punto de acceso
- Estación Wi-fi
- Red Wi-fi abierta
- Red Wi-fi con seguridad habilitada
  - ✔ Nivel físico: intentar que la señal salga lo menos posible de los límites deseados.
  - ✔ Nivel de enlace:

    Controlar el acceso a través de una contraseña común para todos los clientes.
    Controlar el acceso a través de una característica del cliente: MAC y/o nombre de usuario y contraseña.

3.2 WEP

WEP (Wired Equivalent Privacy) es el sistema de cifrado estándar que se utilizó inicialmente para el cifrado del protocolo 802.11.

La principal diferencia entre las redes cableadas e inalámbricas es que en las redes inalámbricas puede intentar entrar en la red cualquier persona dentro del alcance, aunque sea fuera de la empresa, mientras que en una red cableada hay que tener acceso físico a dicha red, es decir, hay que estar dentro de la empresa.

Cuando se utiliza WEP, el punto de acceso y las estaciones de trabajo tienen que compartir una clave (la **clave WEP**).

Se suele hablar de clave WEP de 128 o 64 bits pero en realidad este es el tamaño de la contraseña WEP y el vector distancia (24 bits) juntos. Lo que nos deja 104 bits (13 caracteres) o 40 bits (5 caracteres) para la contraseña WEP.

WEP utiliza un algoritmo llamado **RC4** para a partir de la clave WEP y de un vector de inicialización de 24 bits, genera una secuencia aleatoria llamada semilla, la cual utilizará para cifrar la comunicación con el punto de acceso.

El resultado es una trama en la que la cabecera y el vector de inicialización van sin cifrar y tanto los datos como el CRC van cifrados.

Existen dos métodos a través de los cuales un usuario puede autenticarse con un punto de acceso WEP:

> Abierta (**open**): la estación puede autenticarse sin necesidad de utilizar la clave WEP, simplemente con solicitar la asociación, el punto de acceso dará por asociada a la estación. Después de este proceso de autenticación la estación solamente podrá comunicarse con el punto de acceso si conoce la clave WEP utilizada para cifrar la comunicación.
>
> Clave compartida (**shared key**): cuando una estación envía una solicitud de asociación al punto de acceso, este envía un texto sin cifrar a la estación, llamado “desafío”. El punto de acceso solo asociará a las estaciones que devuelvan correctamente cifrado con la clave WEP dicho texto.

Por motivos de seguridad se recomienda el método de autenticación abierto.

Actualmente el cifrado WEP no se considera seguro (independientemente del tamaño de la clave o el método de autenticación.

WifiSlax (http://www.wifislax.com/manuales.php): software y documentación recomendados para probar ataques (auditar) a la configuración de nuestra Wi-Fi.

3.3 WPA / WPA2

Los estándares WPA (solución intermedia) y WPA2 (solución definitiva) se centran en asegurar el proceso de autenticación y el cifrado de las comunicaciones. En ambos casos se proponen dos soluciones para la autenticación, una empresarial y otra para pequeñas empresas y hogares.

WPA/WPA2 empresarial: requiere de al utilización de un servidor RADIUS independiente para gestionar la autenticación de los usuarios a través de un nombre de usuario y contraseña.

WPA/WPA2 personal: Utiliza un método de autenticación que requiere compartir entre todas las estaciones de la red. Es más apropiado para pequeñas empresas y hogares porque no requiere la utilización de un servidor RADIUS.

3.3.1 WPA / WPA2 PERSONAL

WPA personal utiliza PSK (Pre-Shared-Key) o clave precompartida para el proceso de autenticación.

Con este sistema el administrador asigna una contraseña entre 8 y 36 caracteres en el punto de acceso. Esta contraseña también tiene que introducirse en la configuración de las estaciones inalámbricas que quieran utilizar la red.

Durante el proceso de autenticación se negocia entre las estaciones y el punto de acceso la sucesión de claves que se van a utilizar para cifrar la comunicación posterior. Cada estación negocia su propia clave, por lo que las claves utilizadas por cada estación son diferentes, y además cambian cada cierto tiempo.

Solo durante el proceso de asociación se utiliza la clave compartida.

Para cifrar la comunicación se utiliza la clave que ha negociado la estación y el punto de acceso en el establecimiento de la conexión; y esta contraseña cambia cada cierto tiempo de forma automática.

Existen dos tipos de encriptación en WPA:

TKIP (Protocolo de integridad de clave temporal)

AES (Cifrado avanzado estándar)

Es preferible utilizar AES que TKIP, por ser AES más avanzado y seguro.

No todos los dispositivos Wi-Fi son compatibles con estos estándares; hay que comprobarlo en el punto de acceso y en todas las estaciones que pretendemos conectar.

Actualmente el único ataque posible a este tipo de conexión es el de fuerza bruta, utilizando un diccionario contra los paquetes que se intercambian durante la autenticación. Son especialmente sensibles los puntos de acceso que incluyen contraseñas cortas y contraseñas formadas por palabras y combinaciones de estas.

3.3.1 WPA / WPA2 EMPRESARIAL

El principal inconveniente de todos los sistemas de seguridad inalámbricos anteriores es que es necesario que todas las estaciones de trabajo conozcan la contraseña.

De esta forma es mas fácil (perdida de equipos, ingeniería social, dificultad para el cambio de la contraseña) que la contraseña llegue a quien no deseamos.

Nota: **WirelessKeyWiew** herramienta que permite ver la contraseña wi-fi que tiene configurado el sistema operativo de un equipo.

Arquitectura de una WPA empresarial:

Un **servidor RADIUS** conectado a la red cableada.
Puntos de acceso configurados para utilizar WPA empresarial.
Estaciones Wi-Fi configuradas para utilizar WPA empresarial.

El estándar 802.1x se diseñó para proporcionar autenticación en el nivel de enlace. Por tanto no es algo específico de seguridad Wi-Fi, también puede utilizarse en redes cableadas. Para ello se definen tres elementos:

El **peticionario**: es la estación de trabajo, que está intentando acceder a la red (en nuestro caso Wi-Fi).
El **autenticador**: es el elemento encargado de permitir el acceso o no a un peticionario. En nuestro caso es el punto de acceso.
El **servidor de autenticación**: es el encargado de comprobar la identidad del peticionario y permitir o negar el acceso, informando al autenticador.

Servidor RADIUS sobre Windows 2008 Server:

http://technet.microsoft.com/es-es/library/cc755248%28WS.10%29.aspx

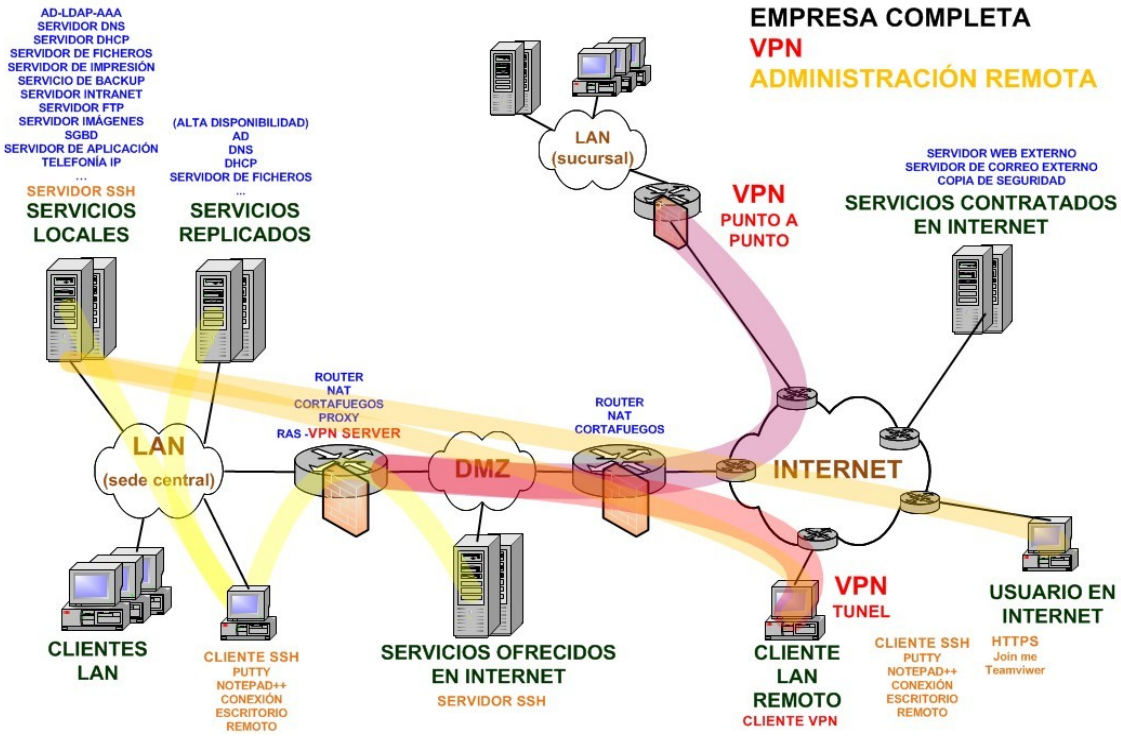
Servidor RADIUS sobre Ubuntu: **Freeradius**

***Ejercicio*: Crear un portal cautivo con Easy Hotspot**

4. VPN

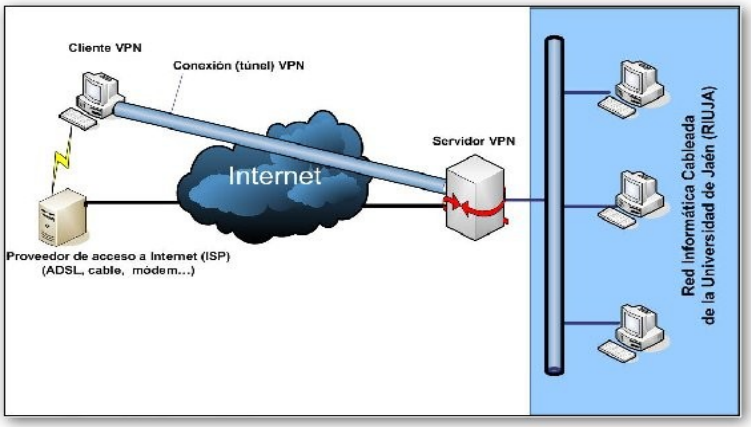
VPN

Comunicar equipos remotos de modo directo es imprescindible en muchas organizaciones, independientemente de donde se encuentren físicamente.



Las redes privadas virtuales (VPN) permiten, mediante el uso de Internet, establecer esta conexión, utilizando protocolos seguros, el acceso a los recursos tiene carácter privado, por lo que una persona podría acceder a los datos de una empresa en la que trabaja con la misma tranquilidad que si se encontrase en su oficina.

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



Las VPN se basan en establecer un **túnel** entre los dos extremos de esta conexión y usar sistemas de cifrado y autenticación para asegurar la confidencialidad e integridad de los datos que se transmiten.

La autenticación en redes virtuales es parecida al sistema de inicio de sesión, utiliza un usuario y su contraseña, por lo que es necesario tener especial cuidado con la seguridad de estos datos. Para mejorar la seguridad algunas empresas utilizan en su VPN un sistema de autenticación basado en claves públicas.

Una vez establecida la conexión, los paquetes de datos se envían encriptados a través del túnel virtual (que se establece sobre Internet). Para cifrar los datos se suelen utilizar claves secretas que solo son válidas mientras dure la sesión.

Formas de conexión en una red VPN

> **Tunneling**: Creamos un túnel sobre Internet utilizando el protocolo SSH. Para este tipo de conexión necesitamos una cuenta en la máquina con la que queremos transmitir los datos. Conexión remota segura.
> **VPN de acceso remoto**: Se trata de acceder a los recursos disponibles desde ubicaciones remotas, utilizando Internet como plataforma de acceso. Realizada la conexión y autenticación del usuario, puede acceder a los mismos recursos que si estuviera presente en la red local de los sistemas a los que accede. Para su implementación necesitamos un cliente VPN en el equipo remoto y un servidor VPN accesible desde Internet en la red local.
> **VPN punto a punto**: Similar al funcionamiento del tunneling, se trata de crear un túnel sobre internet para la transmisión de datos, pero en lugar de aceptar la conexión de un equipo, el servidor VPN acepta la conexión de diversos servidores y sitios, estableciendo el túnel.
> Existe un cuarto tipo VPN interna o **VLAN** con la que conseguimos aislar determinadas zonas de la red local.

Para la implementación de una VPN existen tanto soluciones **hardware** como **software**.

También podemos clasificar las **VPN en función del protocolo que utilizamos** para la realización del túnel:

SSH	VPN a nivel de aplicación
SSL/TLS	VPN a nivel de transporte
IPSec	VPN a nivel de red
PPTP, L2TP, MPLS	VPN a nivel de enlace

Clasificación de las VPN en función del tipo de cifrado: **de clave simétrica o de clave asimétrica**.

La implementación del servidor VPN se realiza sobre un **servidor de acceso remoto (RAS)** en la red de la empresa con acceso desde Internet.

La conexión remota suele apoyarse en servidores de **Autenticación, Autorización y Contabilidad (AAA)** como **RADIUS** o **TACACS+** o en otros servicios de control de acceso como **LDAP**, **EAP**,…

Ejercicio: **Instalación y configuración de una VPN.**

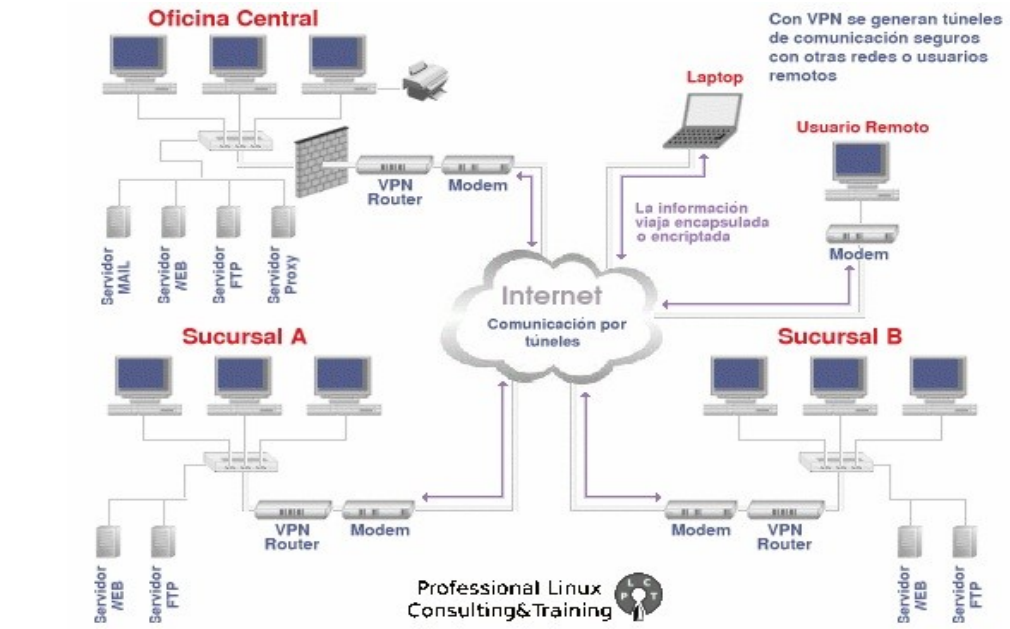
Cuando implementamos una VPN, será necesario realizar la instalación y configuración de dos partes bien diferenciadas, el servidor y el cliente.

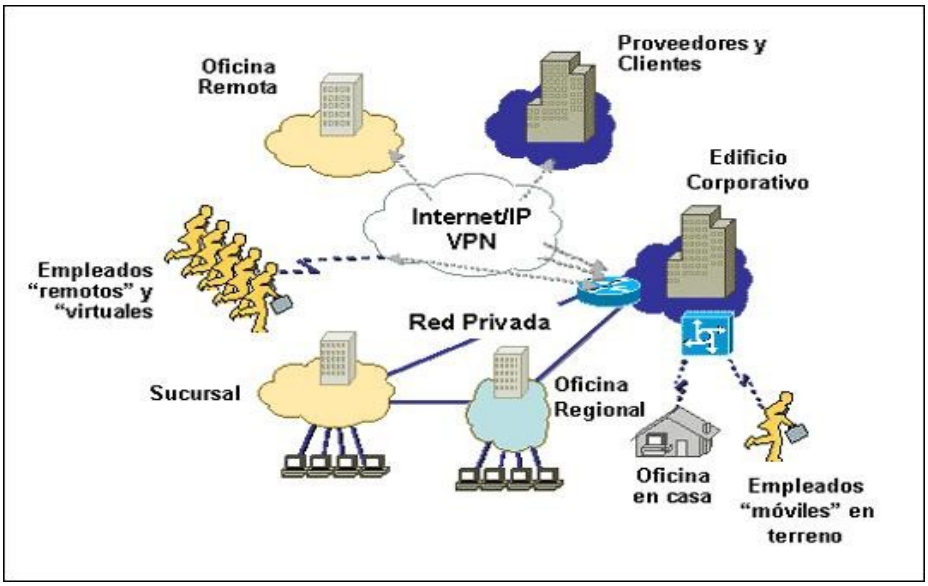
> Implementar un servidor de VPN sobre Windows 2008 server y unir clientes Windows

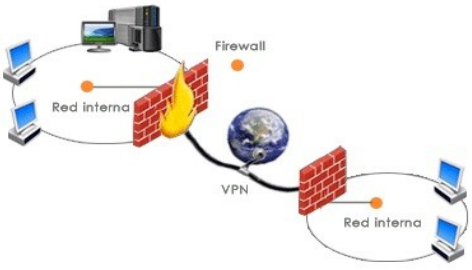
Implementar un servidor de VPN sobre Ubuntu server. OpenVPN

Implementar un cliente de VPN para acceder a la red de la empresa a través de los servidores anteriores.

Crear nuestra propia red VPN en Ubuntu







!! Recordar las herramientas básicas de seguridad activa en redes: ¡¡

TEMA 7 CORTAFUEGOS - TEMA 8 PROXY

ENLACES INTERESANTES - BIBLIOGRAFÍA

Spyware **Antivirus** **Cortafuegos** **Proxy**

Protocolo de comunicaciones **Protocolos de red**

- **HTTPS** **SSH**
- **SSL/TLS**
- **IPSec** **IPv6**
- **WPA** **802.11** **VLAN – 802.1Q**
- **L2TP**

Sistema detector de intrusos (IDS)

Roaming – itinerancia **WDS** **Portal cautivo**

RADIUS **AAA Server** **VPN**

Sniffer **Wireshark** **Nmap**

Nessus **WifiSlax**

Kali linux **Kali linux (wikipedia)**

"Fundamentos de seguridad de redes" – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

"El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

"Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

EJERCICIOS

1. Explica los siguiente conceptos:
Cifrado de comunicaciones como herramienta de seguridad en la red.
Enumera y describe:
Protocolos de **aplicación** que cifran las comunicaciones.
¿Cómo funciona **HTTPS**?
¿Cómo funciona **SSH**?
Protocolos de **transporte** que cifran la comunicación.
Protocolos de **red** que cifran la comunicación
Protocolos de la capa de **acceso a la red** que cifran la comunicación.
Construir un mapa conceptual donde se encuentren los **protocolos de comunicación seguros**, su relación entre ellos, capa del modelo OSI…
Cortafuegos de red como herramienta de seguridad en la red.
Tablas y cadenas de reglas de IPTABLES
Proxy como herramienta de seguridad en la red.
DMZ como herramienta de seguridad en la red. Servicios que la empresa ofrece en Internet.
VPN como herramienta de protección de la red local para intervenciones remotas.

2. Documenta en la red de tu empresa la implementación de la **administración remota segura**:
Administración remota segura de servidores **Linux**
Servidor SSH
Putty
Notepad++
Administración remota segura de servidores **windows**
Administración remota basada en servidores **HTTPS** de Internet (Teamviewer)

3. Cortafuegos **IPTABLES** propuesto para tu empresa
Redirección de puertos para montar el proxy transparente.
Redirección de puertos para permitir la administración remota SSH de un equipo desde Interntet.
Redirección de puertos para llegar al servidor VPN ubicado en la LAN.

4. Configuración correcta del **cortafuegos local** de los equipos de tu empresa. Cortafuegos local habilitado con el mínimo de puertos abiertos, motivando cada uno de los puertos abiertos. Habilitar el protocolo ICMP para permitir las pruebas de conectividad entre los equipos de la empresa.

Avanzado

5. Probar el software **HijackThis** en uno de tus equipos de uso personal, llevar el fichero de log a http://www.hijackthis.de/ e intentar sacar conclusiones sobre los resultados mostrados.

6. Conectarse a un servidor web seguro de Internet y analizar el **certificado** que utiliza.

7. Montar un servidor **HTTPS** sobre Windows 2008 Server.

8. Montar un servidor HTTPS sobre Ubuntu Server.

9. Generar un certificado utilizando **TinyCA** para asociarlo al servidor web seguro de tu empresa.

10. Configura un servidor **SSH** sobre Ubuntu Server. Configura un cliente SSH para realizar una conexión remota a la máquina anterior.

11. Configura un servidor SSH sobre Windows 2008 Server. Configura un cliente SSH para realizar una conexión remota a la máquina anterior.

12. Configura un servidor SSH sobre XP. Configura un cliente SSH para realizar una conexión remota a la máquina anterior.

13. Generar certificados utilizando TinyCA para asociarlo a las cuentas administrador, root, operadordominio, operadorbackup (todas las cuentas que requieran la conexión remota)… en las máquinas de tu empresa en la configuración del servidor SSH y en la configuración de la máquina cliente desde donde se va a realizar la conexión remota segura.

14. Estudio teórico y práctico sobre otras **alternativas de conexión remota** indicando las tecnologías que se utilizan y analizando la seguridad que ofrecen.

15. Utilizar **nmap** para realizar un barrido ping o un rastreo sigiloso sobre la red de tu empresa. Tenga en cuenta si los sistemas se encuentran protegidos por un muro de fuego o no.

16.

17. Utilizar **nessus** para realizar rastreos de vulnerabilidades sobre alguno de los equipos identificados con nmap.

18.

19. Ejercicio Wi-Fi con todas las técnicas de seguridad que permitan los dispositivos utilizados.

20. Estudio teórico sobre el concepto de **portal cautivo**.

21. Estudio teórico sobre el concepto de servidor **RADIUS** y las distintas formas de implementarlo.

22. Relación, utilidad, ventajas e inconvenientes de **LDAP**, **RADIUS** y **Kerberos**.

23. Implementación de un portal cautivo con sevidor RADIUS e itinerancia sobre la Wi-Fi del instituto.

24. Ejercicio **VLAN**. Seguridad en redes locales basada en el switch.

25. Implementación de un servidor **VPN** sobre Windows 2008.

26. Implementación de un servidor VPN sobre Ubuntu Server.

27. Implementación de una VPN que permita trabajar a “jefe1” y “jefe2” desde casa sobre la LAN de la empresa de forma segura.