# Capítulo 6.
# SEGURIDAD EN REDES CORPORATIVAS

Autor: Jesús Costas Santos

# REDES CORPORATIVAS

Índice de contenidos


- 6.1. AMENAZAS Y ATAQUES
  - 6.1.2. Amenazas externas e internas
- 6.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)
- 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED
- 6.4. COMUNICACIONES SEGURAS
  - 6.4.3. VPN
- 6.5. REDES INALÁMBRICAS
  - 6.5.1. SISTEMAS DE SEGURIDAD EN WLAN
  - 6.5.2. RECOMENDACIONES DE SEGURIDAD EN WLAN

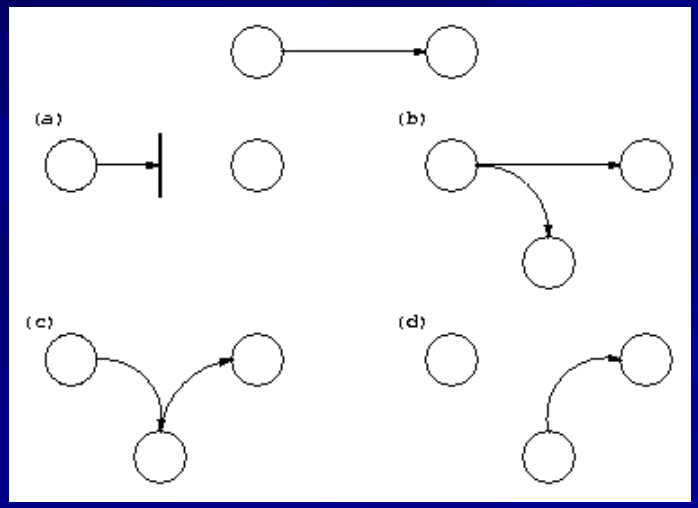
# REDES CORPORATIVAS

## 6.1. AMENAZAS Y ATAQUES

- Redes de ordenadores cada vez son más esenciales para las actividades diarias.
- Ataques e intrusiones a través de las redes públicas y privadas más frecuentes, y pueden causar interrupciones costosas de servicios críticos y pérdidas.
- **Amenazas** en comunicaciones 4 grandes grupos:
  a) **Interrupción**: un objeto, servicio del sistema o datos en una comunicación se pierden, quedan inutilizables o no disponibles.
  b) **Interceptación**: un elemento no autorizado consigue un acceso a un determinado objeto.
  c) **Modificación**: además d el acceso consigue modificar el objeto, es posible incluso la **destrucción**.
  d) **Fabricación**: modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el original y el "fabricado".

# REDES CORPORATIVAS

## 6.1. AMENAZAS Y ATAQUES



# REDES CORPORATIVAS

## 6.1. AMENAZAS Y ATAQUES

- Ejemplos reales de dichas amenazas, **técnicas de ataques informáticos en redes**:
  - **Ataque de denegación de servicio**, también llamado *ataque DoS* (*Deny of Service*), **interrupción** de servicio. Mediante *botnet* o redes zombi controlar máquinas realizar ataques distribuidos de saturación de servidores o DDoS.
  - **Sniffing**, técnica de **interceptación**. Rastrear e interceptar, monitorizando el tráfico de una red.
  - **Man in the middle**, MitM, **interceptación y modificación de identidad**. Supervisión comunicación entre dos partes, falsificando identidades de extremos, recibiendo el tráfico en los dos sentidos.
  - **Spoofing**, **fabricación**, suplantando la identidad o realizando una copia o falsificación de IP, MAC, DNS, web o *mail*. Falsificación de web bancaria: phishing.
  - **Pharming, modificación**. Explotación de una vulnerabilidad servidores DNS o en equipos, modificar las tablas DNS redirigiendo un nombre de dominio (domain name) conocido, a otra máquina (IP) distinta, falsificada y probablemente fraudulenta.

# REDES CORPORATIVAS

## 6.1. AMENAZAS Y ATAQUES

- Software de auditoría de seguridad en redes:
  - Sniffer: Wireshark, Cain & Abel.
  - Spoofing, MitM, Pharming: Cain & Abel.
  - Protección contra MitM: Tablas ARP estáticas, no modificables. Comando: arp –s IP MAC.
  - Monitorizar modificaciones en tablas ARP: Wireshark, o sistema de detección de intrusos (IDS) como SNORT.

# REDES CORPORATIVAS

Índice de contenidos


- 6.1. AMENAZAS Y ATAQUES
  - 6.1.2. Amenazas externas e internas
- 6.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)
- 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED
- 6.4. COMUNICACIONES SEGURAS
  - 6.4.3. VPN
- 6.5. REDES INALÁMBRICAS
  - 6.5.1. SISTEMAS DE SEGURIDAD EN WLAN
  - 6.5.2. RECOMENDACIONES DE SEGURIDAD EN WLAN

# REDES CORPORATIVAS

## 6.1.2. Amenazas externas e internas

- Las amenazas de seguridad en redes corporativas o privadas de una organización, originarse:
  - **Amenaza externa o de acceso remoto**: atacantes externos a la red privada o interna de una organización, y se introducen desde redes públicas. Los objetivos servidores y *routers* accesibles desde el exterior, y pasarela de acceso a la redes corporativa.
  - **Amenaza interna o corporativa**: los atacantes acceden sin autorización o pertenecen a la red privada de la organización.
- Contra dichas amenazas: Defender la **seguridad en la red corporativa** de forma interna (capítulo 6), y medidas de **protección perimetral** (capítulo 7), en equipos expuestos a redes públicas.

# REDES CORPORATIVAS

## 6.1.2. Amenazas externas e internas

- Para protegernos de las posibles **amenazas internas** propuestas:
  - Diseño de direccionamiento, parcelación y servicios de subredes dentro de nuestra red corporativa. Subnetting, VLAN y DMZ.
  - Políticas de administración de direccionamiento estático para servidores y *routers*.
  - Monitorización del tráfico de red y de las asignaciones de direccionamiento dinámico y de sus tablas ARP.
  - Modificación de configuraciones de seguridad, contraseñas por defecto de la administración de servicios.
  - En redes inalámbricas emplear máximo nivel de seguridad.

# REDES CORPORATIVAS

## 6.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

- Herramienta de seguridad detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.
- Buscan patrones previamente definidos que impliquen actividad sospechosa o maliciosa sobre nuestra red o *host*, aportan capacidad de prevención y de alerta anticipada.
- Los **tipos** de IDS que encontramos son:
  - HIDS (*Host* IDS): protegen un único servidor, PC o *host*.
  - NIDS (Net IDS): protege un sistema basado en red. Capturando y analizando paquetes de red, es decir, son *sniffers* del tráfico de red.

# REDES CORPORATIVAS

## 6.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

- La arquitectura de un IDS, a grandes rasgos, está formada por:
  - La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o IDS *host*, el propio sistema.
  - Reglas y filtros sobre los datos y patrones detectar anomalías.
  - Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía *mail*, o SMS.
- Ubicación del IDS: uno delante y otro detrás de cortafuegos perimetral de nuestra red.
- Ejemplo: Windows y GNU/Linux:
  - SNORT: *sniffer*, registro de paquetes, logs para su posterior análisis, o NIDS.
  - Ej: snort -dev -l ./log -h 192.168.1.0/24 -c ../etc/snort.conf.
  - snort.conf: configuración de las reglas, preprocesadores y otras funcionamiento en modo NIDS.

# REDES CORPORATIVAS

## 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

- TCP/IP arquitectura de protocolos usan ordenadores para comunicarse en red.
- **Puertos de comunicaciones** o **numeración lógica: identificar cada una de las conexiones de red**, **origen y destino**.
- Los servicios de red más habituales: *puertos bien conocidos*:
  - 80 HTTP o web
  - 20-21 para transferencia de ficheros FTP
  - 23 para administración remota en modo comando TELNET.
- Sistemas y sus aplicaciones de red, ofrecen y reciben servicios a través de dichos puertos de comunicaciones.

# REDES CORPORATIVAS

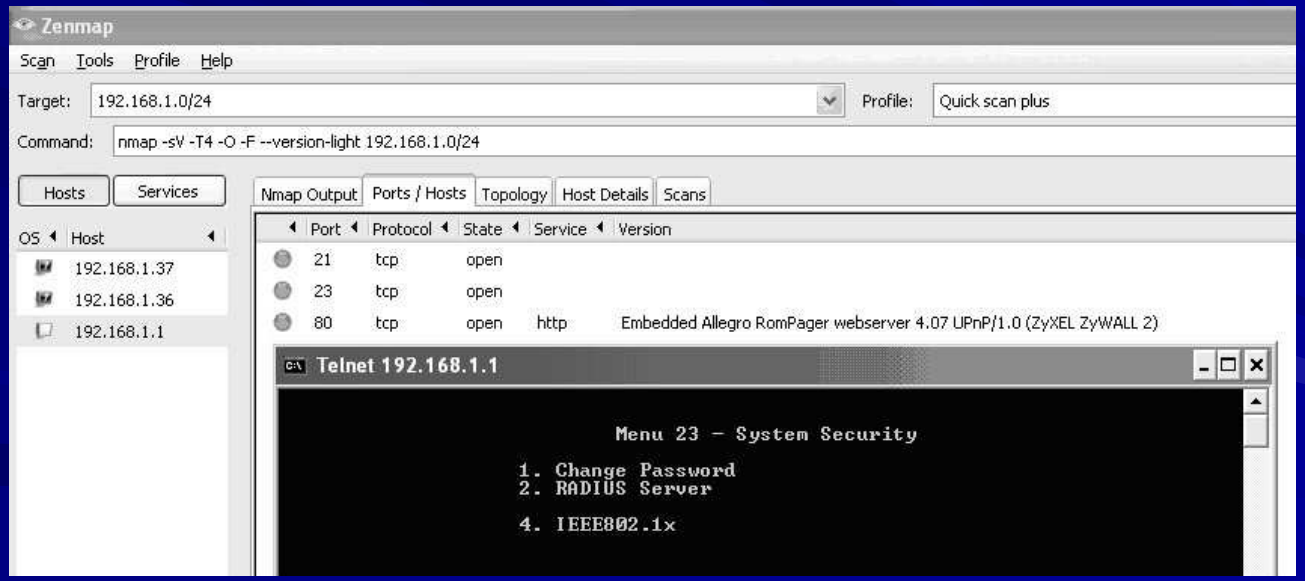
## 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

- El análisis y control de los puertos se pueden realizar desde distintos frentes:
- En una **máquina local** conexiones y puertos abiertos y aplicaciones controlan.
  - El comando **netstat** permite ver el estado en tiempo real de nuestras conexiones.
  - Los **cortafuegos o** *firewall* **personales** protección frente a ataques externos.
- En la **administración de red** puertos y en qué estado un conjunto de equipos.
  - La aplicación **nmap** permite un escaneo de puertos, aplicaciones y sistemas operativos, en un rango de direcciones.
  - Los **cortafuegos y proxys perimetrales** ofrecen protección mediante un filtrado de puertos y conexiones hacia y desde el exterior de una red privada.
- Tras realizar un análisis exhaustivo a nivel de puertos, debemos proteger nuestras conexiones, haciéndolas seguras, por ejemplo cuando enviemos información confidencial.

# REDES CORPORATIVAS

## 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

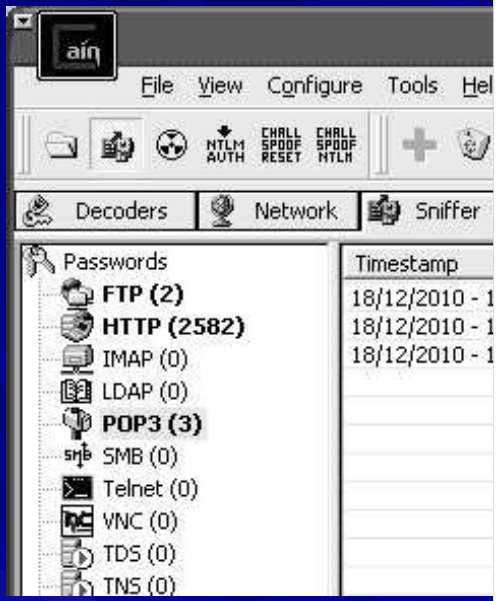
- Análisis de puertos y aplicaciones de red, en 192.168.1.0/24 con NMAP (aplicación gráfica ZENMAP).



# REDES CORPORATIVAS

## 6.4. COMUNICACIONES SEGURAS

- Comunicaciones: HTTP, FTP o SMTP/POP, no emplean cifrado en las comunicaciones. Cain & Abel capacidad de recuperar tráfico y contraseñas de dichos protocolos.
- Protocolos que emplean comunicaciones cifradas:
  - **SSH** puerto 22, envío seguro de archivos mediante SFTP.
  - **SSL y TLS**: *Secure Sockets Layer* -Protocolo de Capa de Conexión Segura- (**SSL**) y *Transport Layer Security* -Seguridad de la Capa de Transporte- (**TLS**), su sucesor. Capa entre aplicación y sobre transporte TCP. Entre otros se emplea a través de puertos específicos con: HTTPS , FTPS, SMTP, POP3, etc.
  - **IPSEC** o *Internet Protocol security*, conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. Actúan en la capa 3 puede ser utilizado protocolos de la capa 4, TCP y UDP.



# REDES CORPORATIVAS

## 6.4.3. VPN

- Una red privada virtual o VPN (*Virtual Private Network*): tecnología de red **extensión de una red local** de forma segura sobre una red pública, como Internet.
- Ejemplo: conectar utilizando Internet, dos o más sucursales de una empresa, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de trabajo, etc.
- Para hacerlo de **manera segura** garantizar:
  - **Autenticación y autorización**: controlan los usuarios y/o equipos y qué nivel de acceso debe tener.
  - **Integridad**: los datos enviados no han sido alterados, funciones resumen o hash, como MD5 y SHA.
  - **Confidencialidad**: Algoritmos de cifrado como DES, 3DES y AES.
  - **No repudio**: mensajes firmados.

# REDES CORPORATIVAS

## 6.4.3. VPN

- 3 **arquitecturas de conexión VPN**:
  - **VPN de acceso remoto**: más usado, usuarios o proveedores se conectan con la empresa desde sitios remotos Internet como vínculo de acceso.
  - **VPN punto a punto**: servidor VPN, posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. **Tunneling.**
  - **VPN over LAN**: es el menos difundido. Sobre LAN de la empresa, aisla zonas y servicios de la red interna, añadir cifrado y autenticación mediante VPN.
- Protocolo estándar VPN: IPSEC.
- También: PPTP, L2TP, SSL/TLS, SSH, etc. 2 de las tecnologías más utilizadas:
  - **PPTP** o *Point to Point Tunneling Protocol*: protocolo Microsoft. Sencillo y fácil de implementar menor seguridad que L2TP.
  - **L2TP** o *Layer Two Tunneling Protocol*: estándar abierto y disponible en la mayoría de plataformas Windows, Linux, Mac, etc. Sobre IPSec y altos niveles de seguridad.
- Ejemplo conexiones remotas: Windows y GNU/Linux Logmein Hamachi: crea red privada entre host remotos.

# REDES CORPORATIVAS

## 6.5. REDES INALÁMBRICAS

- **Comunicaciones inalámbricas** o *wireless* **ventajas** contra cable:
  - **Conectividad en cualquier momento y lugar**, es decir mayor disponibilidad y acceso a redes.
  - **Instalación simple y económica**.
  - Fácilmente **escalable**.
- **Riesgos y limitaciones**.
  - Rangos del espectro de radiofrecuencia (RF) **sin costes de licencia** por su transmisión y uso. Rangos saturados e interferencias
  - **Poca seguridad**. Cualquier equipo con tarjeta de red inalámbrica interceptar cualquier comunicación de su entorno.
- Mejoras continuas en **encriptación** y la **autenticación**.
- Comunicaciones cableadas (fibra, cable de pares, coaxial) medios de acceso físico más seguros que existen en la actualidad.

# REDES CORPORATIVAS

## 6.5.1. SISTEMAS DE SEGURIDAD EN WLAN

- Los sistemas de cifrado autenticación + encriptación en redes inalámbricas son:
  - **Sistema abierto** u *Open System*: sin autenticación en el control de acceso a la red, realizado por el punto de acceso, ni cifrado en las comunicaciones.
  - **WEP** o *Wired Equivalent Privacy* o Privacidad Equivalente a Cableado: sistema estándar en la norma 802.11. Encriptación de los mensajes claves de 13 (104 bits) o 5 (40 bits) caracteres, también denominadas WEP 128 o WEP 64 respectivamente. Autenticación existen 2 métodos:
    - **Sistema abierto** u Open system, el cliente no se tiene que identificar en el Punto de Acceso durante la autenticación. Después de la autenticación y la asociación a la red, el cliente tendrá que tener la clave WEP correcta para descifrar mensajes enviados y recibidos.Modo recomendado.
    - **Claves precompartida**, Pre-Shared Keys o PSK. Se envía la misma clave de cifrado WEP para la autenticación, verificado por el punto de acceso.
- Es aconsejable usar la autenticación de sistema abierto para la autenticación WEP, es posible averiguar la clave WEP interceptando los paquetes de la fase de autenticación.

# REDES CORPORATIVAS

## 6.5.1. SISTEMAS DE SEGURIDAD EN WLAN

- **WPA** o **Wi-Fi Protected Access o Acceso Protegido Wi-Fi**: corregir las deficiencias del sistema previo WEP. 2 publicaciones WPA, y definitivo WPA2 estándar 802.11i.

- Se proponen 2 soluciones según el ámbito de aplicación:
  - **WPA Empresarial** o WPA-Enterprise (grandes empresas): autenticación mediante un servidor RADIUS, almacenan las credenciales y contraseñas de los usuarios de la red.
  - **WPA Personal** (pequeñas empresas y hogar): autenticación mediante clave precompartida, similar al WEP.
- Mejoras de WPA sobre WEP: protocolo de integridad de clave temporal (**TKIP** - *Temporal Key Integrity Protocol*), **cambia claves dinámicamente** a medida que el sistema es utilizado.

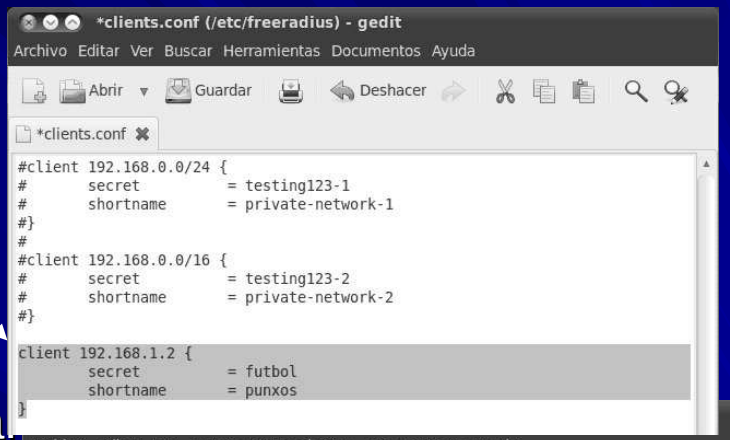
- Mayor nivel de seguridad en el cifrado, con algoritmo de cifrado simétrico **AES**, más robusto y complejo que **TKIP**, su implementación HW más potente, no se encuentra disponible en todos los dispositivos.
- WPA sistema más seguro, problema: compatibilidad y disponibilidad de las distintas versiones y algoritmos de cifrado del mismo en los dispositivos de una misma red.

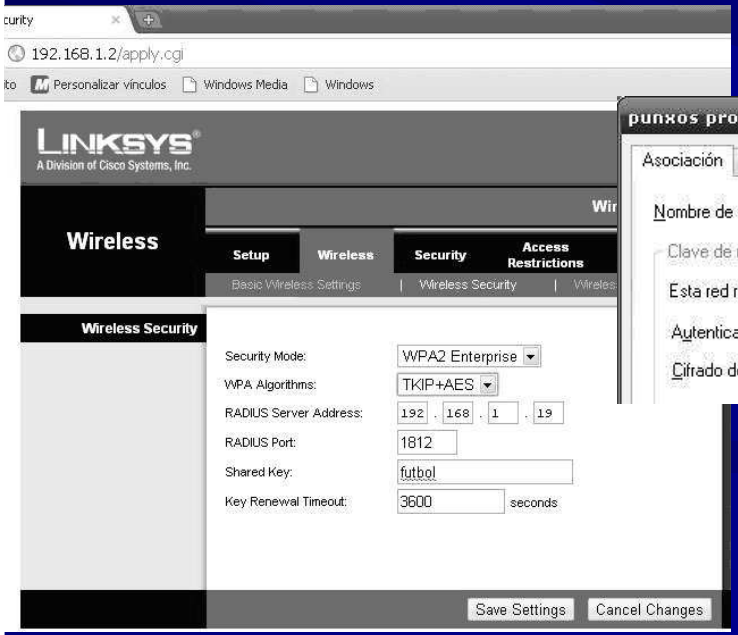
# REDES CORPORATIVAS

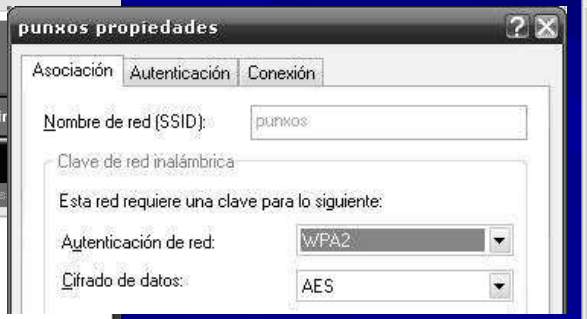
## 6.5.1. SISTEMAS DE SEGURIDAD EN WLAN

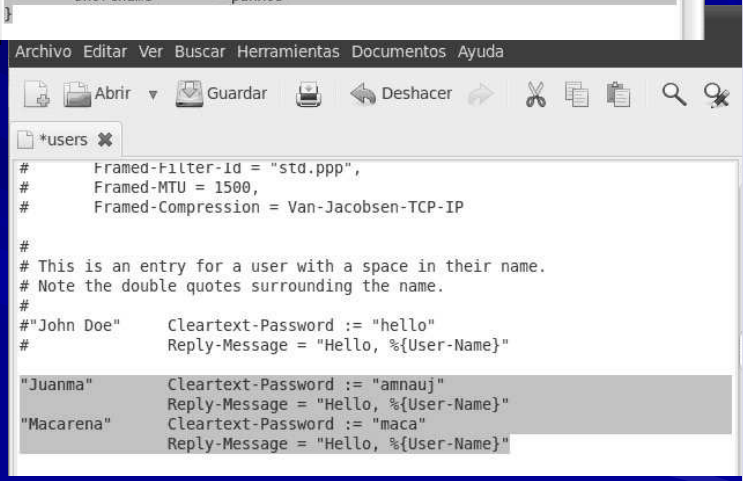
WPA2 Enterprise o empresarial:

1. Configurar Servidor Radius (ej:Feeradius)
2. Asociar punto de acceso a servidor de autenticación RADIUS
3. Configurar cliente o tarjeta de red inalámbrica



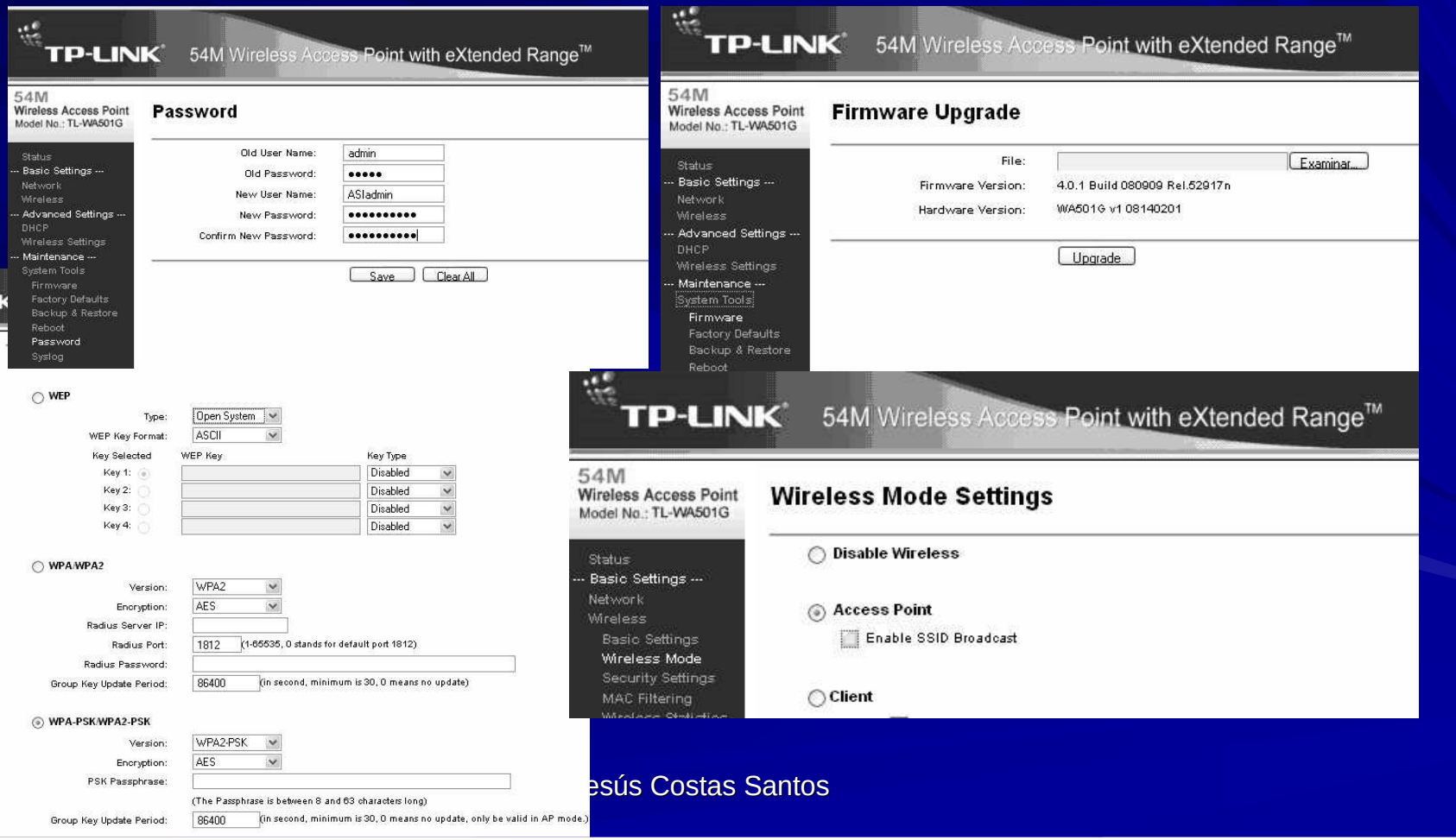
# REDES CORPORATIVAS

## 6.5.2. RECOMENDACIONES DE SEGURIDAD EN WLAN

- Acceso a redes inalámbricas punto muy débil de seguridad en redes corporativas:
  1. Asegurar la administración del punto de acceso (AP), punto de control de las comunicaciones de todos los usuarios, crítico en la red, cambiar la contraseña por defecto.
  2. Actualizar el firmware disponible mejorar sus prestaciones de seguridad.
  3. Aumentar la seguridad de los datos transmitidos: encriptación WEP o WPA/WPA2 o servidor Radius, y cambiando las claves regularmente.
  4. Realizar una administración y monitorización minuciosa, administración + compleja de clientes, pero + segura:
     1. Cambia el SSID por defecto y desactiva el broadcasting SSID. Clientes deberán conocer el nombre del SSID.
     2. Desactivar el servidor DHCP, manualmente las direcciones IP en clientes.
     3. Cambiar las direcciones IP del punto de acceso y el rango de la red por defecto.
     4. Filtrado de conexiones permitidas mediante direcciones MAC.
     5. Número máximo de dispositivos que pueden conectarse.
     6. Analizar periódicamente los usuarios conectados verificando si son autorizados o no.
  5. Desconexión del AP cuando no se use.

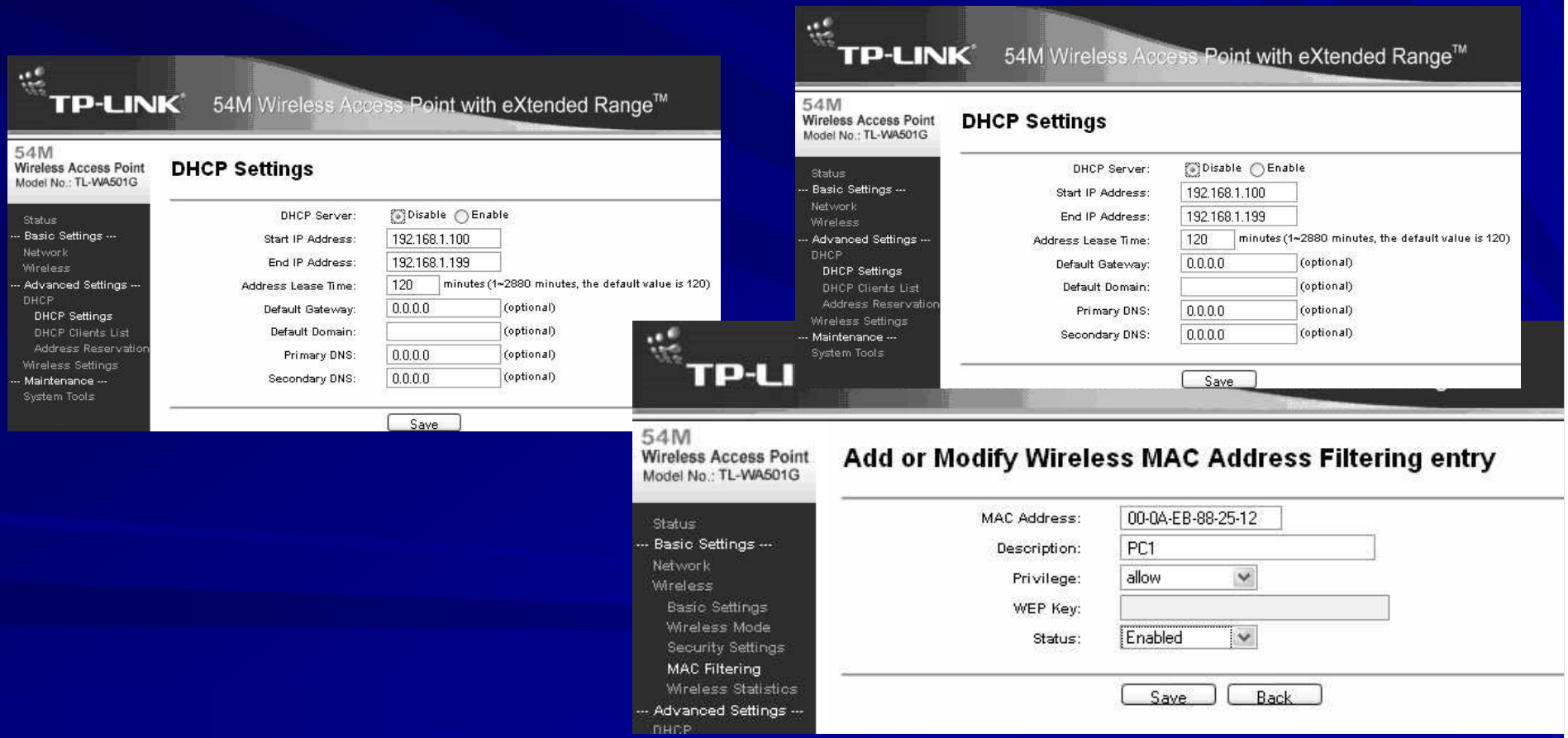
# REDES CORPORATIVAS

## 6.5.2. RECOMENDACIONES DE SEGURIDAD EN WLAN



# REDES CORPORATIVAS

## 6.5.2. RECOMENDACIONES DE SEGURIDAD EN WLAN



# REDES CORPORATIVAS

## DIRECCIONES DE INTERÉS

- Curso abierto con materiales y ejercicios sobre Seguridad Avanzada en Redes
  - http://ocw.uoc.edu/informatica-tecnologia-y-multimedia/aspectos-avanzados-de-seguridad-en-redes/Course_listing
- Sitio web sobre seguridad informática en materia de redes:
  - http://www.virusprot.com/
- Noticias sobre seguridad en redes. Asociación de internautas:
  - http://seguridad.internautas.org/
- Conexiones inalámbricas seguras y auditorías wireless en:
  - http://www.seguridadwireless.net/
- Blog especializado en seguridad y redes
  - http://seguridadyredes.nireblog.com/

# REDES CORPORATIVAS

**DIRECCIONES DE INTERÉS**

- **Escaneo de puertos on-line**
  - http://www.internautas.org/w-scanonline.php
  - http://www.upseros.com/portscan.php
  - http://www.kvron.com/utils/portscanner/index.php
- **Test de velocidad de tu conexión a Internet**
  - http://www.adsl4ever.com/test/
  - http://www.testdevelocidad.es/
  - http://www.internautas.org/testvelocidad/
  - http://www.adslayuda.com/test-de-velocidad/
- **Test sobre phishing de Verisign disponible en**
  - https://www.phish-no-phish.com/es

# REDES CORPORATIVAS

## SOFTWARE-SIMULADORES

- Simuladores de configuración de dispositivos como router-punto de acceso inalámbrico TP-LINK.
  - http://www.tp-link.com/support/simulator.asp
  - http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm
- Simulador del router inalámbrico Linksys WRT54GL:
  - http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm
- Simuladores de routers inalámbricos D-Link:
  - http://support.dlink.com/emulators/dwlg820/HomeWizard.html
  - http://support.dlink.com/emulators/dsl2640b/306041/vpivci.html
  - http://support.dlink.com/emulators/dwl2100ap
  - http://support.dlink.com/emulators/di604_reve

# REDES CORPORATIVAS

**SOFTWARE**

- Angry IP Scanner : software escaneador de IP.
  - http://www.angryip.org/w/Download
- Wireshark: Packet sniffer:
  - http://www.wireshark.org/download.html
- Cain & Abel: sniffer, generador de ataques MitM, spoofing, etc.
  - http://www.oxid.it/cain.html
- SNORT: software de detección de intrusos (IDS).
  - http://www.snort.org/
- Alarmas de intentos de duplicados ARP: bajo GNU/Linux Arpwatch o en Windows DecaffeinatID
  - Arpwatch: http://freequaos.host.sk/arpwatch/
  - DecaffeinatID: http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows
- Openssh-server: servidor de SSH.
  - http://www.openssh.com/
- Putty: cliente SSH bajo sistemas Windows.
  - http://www.putty.org/
- Filezilla Server y Client: cliente y servidor FTP.
  - http://filezilla-project.org/

# REDES CORPORATIVAS

## SOFTWARE

- Logmein Hamachi: software de conectividad P2P y VPN entre equipos remotos.
  - www.logmein.com
- Backtrack: distribución específica con un conjunto de herramientas de auditorías de seguridad, entre otras algunas que permiten escalada de privilegios en sistemas Windows (ophcrack) y GNU/Linux (John the ripper).
  - http://www.backtrack-linux.org/
- Wifiway y Wifislax: distribuciones orientadas a realizar auditorías wireless, como recuperación de contraseñas. En las últimas versiones incluyen Minidwep-gtk.
  - www.wifiway.org/
  - http://www.wifislax.com/
- Opewrt: distribución de actualización del firmware para routers y puntos de acceso inalámbricos. Se recomienda siempre realizar previamente una copia de seguridad del firmware actual.
  - http://openwrt.org/
- AlienVault: software libre de administración y monitorización de redes.
  - http://alienvault.com/
- FreeRadius: servidor Radius, de software libre.
  - http://freeradius.org/

# REDES CORPORATIVAS

## NOTICIAS

- Tabnabbing; phishing a través de las pestañas del navegador
  - Fuente: http://www.hispasec.com/unaaldia/4231
- Artículo de pintura antiwifi de EM-SEC Technologies. Puede leer sobre dicha pintura en:
  - http://www.publico.es/ciencias/273942/una-pintura-protege-a-los-navegantes-de-los-intrusos/version-imprimible