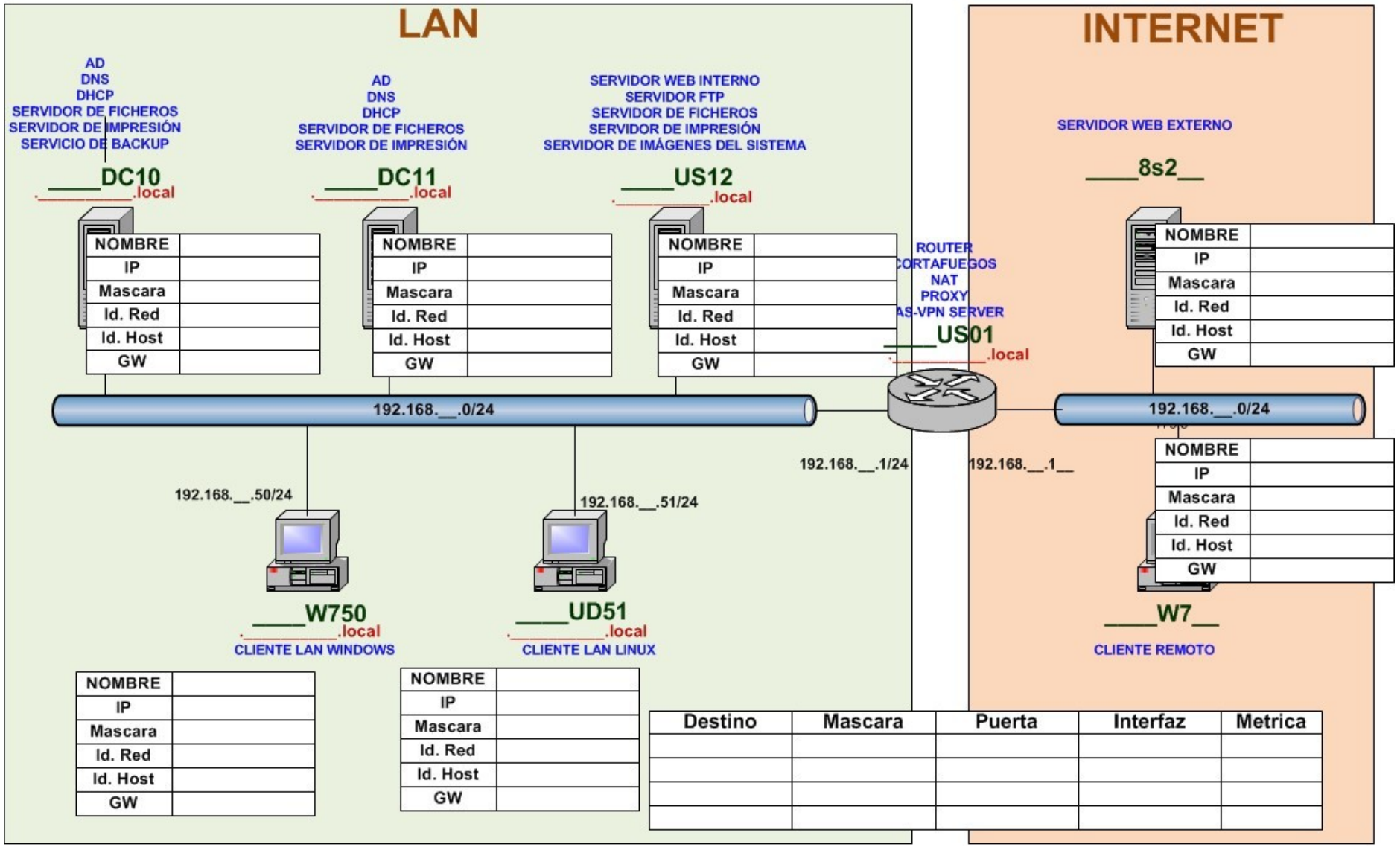
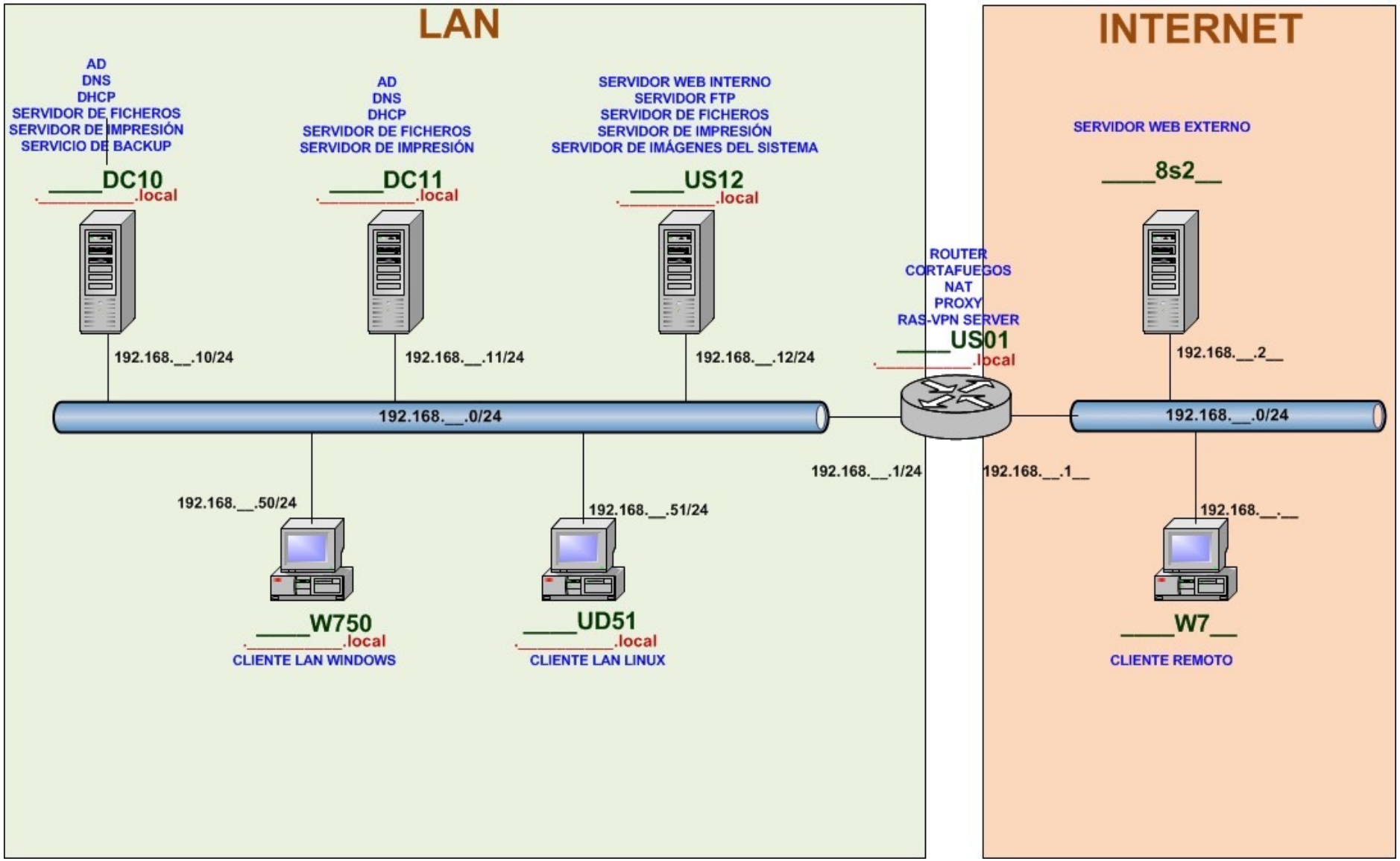
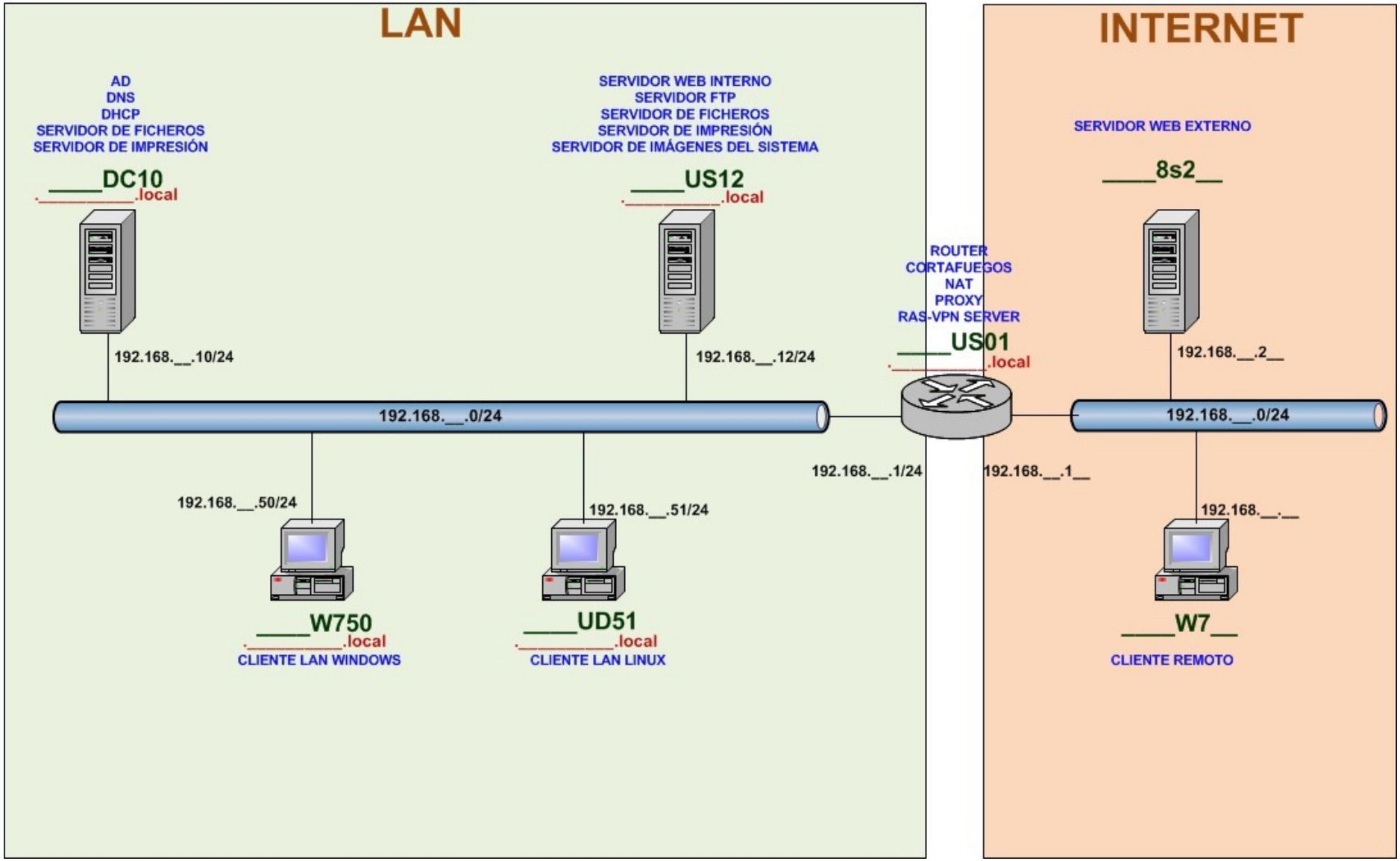
MODELO DE REFERENCIA



MODELO GRADO SUPERIOR EMPRESA _____



MODELO GRADO MEDIO EMPRESA _____



Consideraciones generales

El modelo utilizado será el mismo para todos los ejercicios del curso.

Cada uno de los equipos representados en el modelo serán implementados por el alumno con una máquina virtual distinta. En el caso de que una máquina se deteriore durante la realización del ejercicio, el alumno deberá sustituirla por otra máquina limpia y retomar el ejercicio donde sea necesario para conseguir los objetivos del ejercicio.

Cada ejercicio puede requerir la utilización de una o varias máquinas virtuales del modelo en función de la técnica de seguridad que estemos practicando. No es necesario entregar las máquinas virtuales, pero si deben estar correctamente configuradas en el equipo del alumno para que el profesor pueda, en un momento dado, comprobar la autenticidad de la documentación entregada y la correcta configuración de la máquina del alumno. Es responsabilidad del alumno disponer de copias de seguridad de máquinas y ficheros de configuración que le permitan recuperarse de un desastre.

Todas las máquinas utilizadas en la práctica deberán ser convenientemente documentadas sobre un **documento de texto** como prueba de su realización y como manual de instalación para posteriores implementaciones de la técnica. La documentación podrá ser realizada en varios documentos pero agrupada y ordenada convenientemente siguiendo la secuenciación de las actividades del curso y los títulos indicados en este guión.

El alumno dispondrá de un documento general de “empresa” donde recogerá los planos de red y las decisiones que posteriormente se implementarán en las máquinas de la empresa.

El alumno documentará ademas los scripts desarrollados y las copias de ficheros de configuración necesarios.

Cada alumno utilizará una dirección de red para su LAN distinta a la del resto de compañeros; la red que utilizaremos para simular Internet será común a todos los alumnos.

En general, los ejercicios se realizarán teniendo en cuenta que van a estar dirigidos a una **pequeña empresa de 5-20 puestos cliente y 2-4 servidores** con las siguientes consideraciones:

- Los usuarios de los equipos cliente utilizarán los servidores para almacenar la información de la empresa.
- Los servidores ofrecerán a los equipos cliente todos los servicios estudiados en cada momento garantizando la mayor disponibilidad posible en función de las características de la empresa.
- La empresa dispone de una salida a interne a través de una línea ADSL.
- En todos los equipos utilizaremos software legal.

Los ejercicios prácticos estarán agrupados en tres bloques:

- **Seguridad en el cliente (septiembre-octubre)**
- **Seguridad en el servidor y en la LAN (noviembre-diciembre)**
- **Seguridad en la conexión a Internet (enero-febrero)**

Nos referiremos a estos bloques como **Examen práctico 1, 2 y 3.**

La evaluación de estos ejercicios es continua, ya que las técnicas desarrolladas en un bloque se basan en el funcionamiento del las técnicas del bloque anterior.

Examen práctico 1: Seguridad en el cliente

Sobre Windows y Linux Desktop

- Seguridad física: presupuesto y características.
- Seguridad lógica: asegurar un cliente de uso compartido conectado a Internet
- Monitor de seguridad – Análisis de vulnerabilidades
  - ✗ Wireshark
  - ✗ Nmap
  - ✗ Nessus

Examen práctico 2: Seguridad en el servidor y en la LAN

Sobre Windows / Ubuntu server / CentOS / FreeNAS / Proxmox / ...

- RAID
- SSH – Administración remota segura – Escritorio remoto de Windows
- DHCP

- DNS
- AD
- NFS
- DFS
- Backup
- Virtualización
- Servidor de impresión
- HTTPS
- FTP / SFTP
- Servidor de imágenes
- Portal cautivo – WPA empresarial – RADIUS

Examen práctico 3: Seguridad en la conexión a Internet

Sobre Windows / Ubuntu server / CentOS / FreeNAS / Proxmox / ...

- Router
- NAT
- Cortafuegos
- Proxy
- VPN – Sede central / Sucursal – Cliente on-line
- DMZ
- Contratar servicios en internet
- Ofrecer servicios en internet
- Cifrado de las comunicaciones: WPA, IPSec, SSL/TLS, IPv6…
- IDS

EXAMEN PRÁCTICO 1: SEGURIDAD EN EL CLIENTE

SEGURIDAD FÍSICA: PRESUPUESTO Y CARACTERÍSTICAS

Imaginemos que tenemos que encargarnos de la compra de los equipos necesarios para nuestra pequeña empresa y nos han pedido una estimación del presupuesto necesario; realizar una propuesta para presentar a la dirección de la empresa.

Dispositivo (hardware y software necesario)

Características u utilidad del dispositivo

Presupuesto

Fabricante y proveedor

SEGURIDAD LÓGICA SOBRE UN CLIENTE

Utilizando una máquina virtual para cada uno de los distintos sistemas operativos que manejen los clientes de nuestra empresa (mínimo Windows 7 y Ubuntu Desktop).

Para la realización de este ejercicio suponemos que se trata de un equipo cliente conectado a Internet cuyo uso va a ser compartido por varios usuarios y, en ocasiones, deberá compartir información con otro equipo cliente de la misma LAN.

El alumno debe presentar una propuesta de configuración segura de sus clientes que incluya al menos:

Identificación de los equipos de la empresa.

Configuración de red de los equipos de la empresa.

Cuentas locales de los equipos cliente.

Cortafuegos local.

Antivirus.

Configuración segura de la BIOS.

Configuración segura de los dispositivos y puertos de entrada.

Configuración segura de los navegadores utilizados.

Configuración de los recursos compartidos con usuarios locales.

Configuración de los recursos compartidos con usuarios de otro equipo cliente.

Cifrado de información.

Control de acceso de los usuarios locales a las aplicaciones.

Control de acceso de los usuarios locales a Internet.

Copia de seguridad de datos (comprimida y cifrada)

Recuperación de una copia de seguridad de datos total o parcial.

Imagen del sistema.

Recuperación de una imagen del sistema.

Equipos con varios sistemas.

Equipos con varios sistemas y un espacio de disco compartido.

RAID.

Virtualización de clientes.

Congelación de equipos.

Punto de información.

Sugerencias para mejorar este ejercicio.

MONITOR DE SEGURIDAD

Preparar una máquina virtual desde la que podamos entrenar todas las herramientas de seguridad que vamos viendo durante el curso.

Elegir y motivar la elección del sistema operativo de esta maquina.

Identificador de host del monitor de seguridad (52)

Identificador de host del equipo atacante (53)

Instalar y probar las herramientas que vamos viendo a lo largo del curso.

Wireshark

Nmap

Nessus

22 Pasos para aumentar la seguridad de la red: http://openwebinars.net/22-pasos-para-aumentar-la-seguridad-de-tu-red/

Kali Linux	http://www.kali.org/
BackTrack Linux	http://www.backtrack-linux.org/

EXAMEN PRÁCTICO 1: SEGURIDAD LÓGICA SOBRE UN CLIENTE - DETALLE

OBJETIVO:

El objetivo del ejercicio es la puesta en práctica de aspectos relacionados con la seguridad informática en un ordenador personal con conexión a Internet y utilizado por varios usuarios.

1. PUNTO DE PARTIDA EXAMEN PRÁCTICO 1

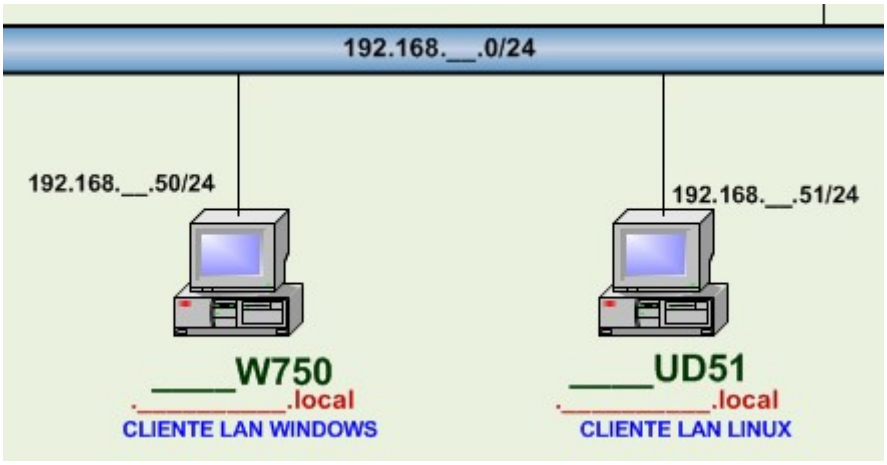
Maquinas virtuales Oracle Virtual Box

xxx-W750 Windows 7 Professional / Windows X Professional

xxx-UD51 Linux Mint

Windows y Linux en la misma máquina

xxx-MS52 Máquina utilizada como monitor de seguridad



NOTA: el alumno puede utilizar otros sistemas operativos (a mayores) en las máquinas cliente de su empresa.

NOTA2: el enunciado es válido para todas las máquinas virtuales cliente.

2. IDENTIFICACIÓN DEL EQUIPO Y CONFIGURACIÓN INICIAL

Identificación del equipo, grupo de trabajo y configuración de red.

Nombre de equipo: **xxx-W750** / **xxx-UD51** / **xxx-MS40**

Grupo de trabajo: **IS22**

IP: **192,168.5.(host del aula +100 para W7 y +200 para Linux)**

GW: **192.168.5.1**

DNS: **8.8.8.8**

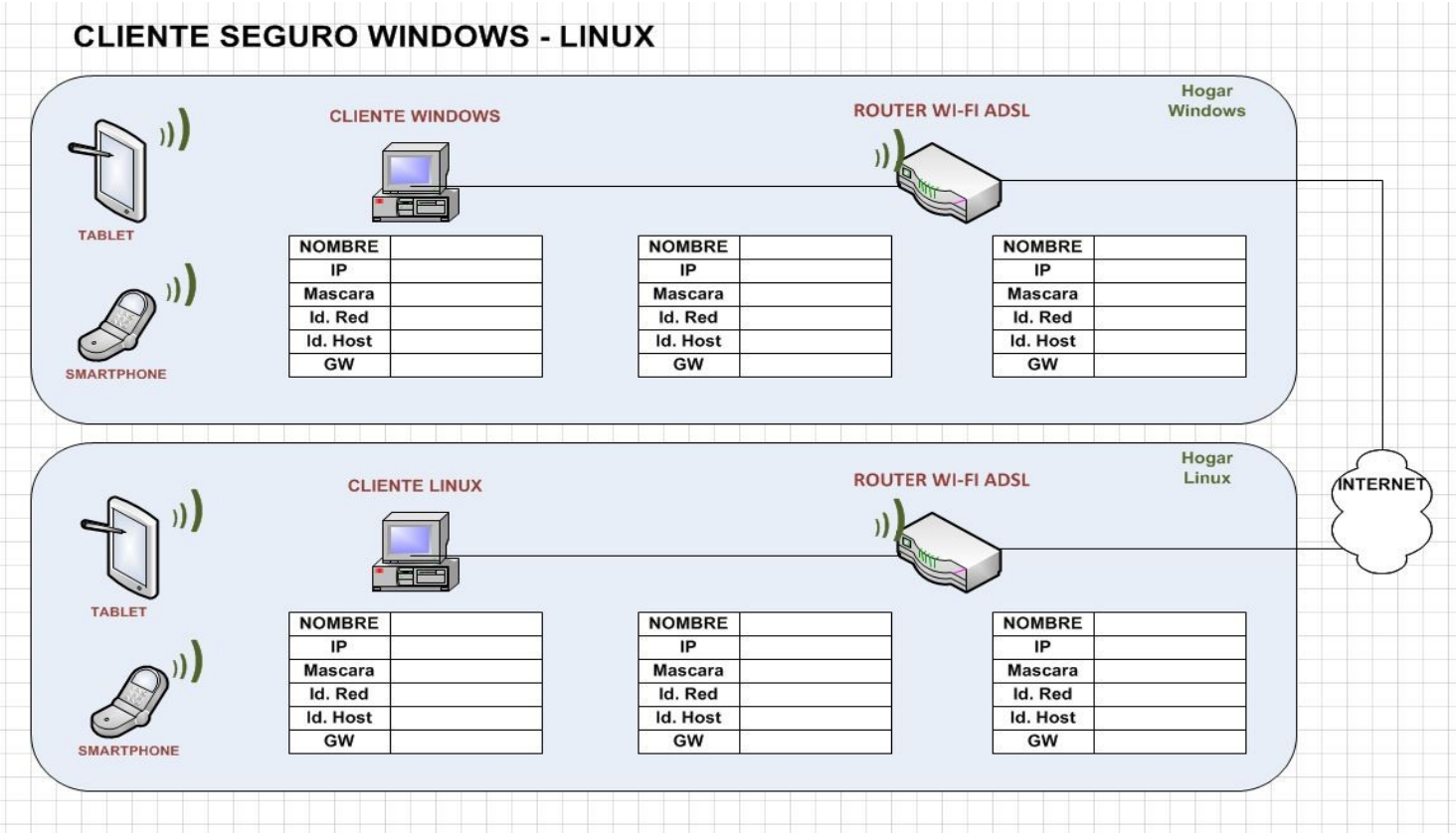
Nota1: la utilización del grupo de trabajo del aula es provisional hasta que pongamos en funcionamiento el dominio de AD de la empresa (examen práctico 2), momento a partir del cual los equipos cliente pasarán a incluirse en el dominio de la empresa.

Nota2: la utilización de la red del aula es provisional hasta que pongamos en funcionamiento el router de la empresa, momento a partir del cual debemos cambiar la configuración de red de los equipos cliente utilizando la configuración de red, la puerta de enlace y servidor DNS correspondiente.

ALTERNATIVA DE CONFIGURACIÓN

Utilizando un router wi-fi para disponer de una red independiente para el equipo que estamos configurando, lo que nos permitirá probar y documentar:

- Seguridad del router wi-fi
- Seguridad de la red Wi-fi
- Seguridad en la configuración y uso de dispositivos Android
- Seguridad en la configuración y uso de dispositivos Windows
- Seguridad en la configuración y uso de dispositivos Linux



3. CUENTAS DE USUARIO LOCALES

miadmin / P@ssw0rd	administrador del equipo (Linux)
administrador/P@ssw0rd	administrador del equipo (Windows)
miadmin2/ P@ssw0rd	administrador del equipo
*nombre***/ P@ssw0rd**	usuario normal en función del enunciado
*hermanonombre***/ P@ssw0rd**	usuario restringido en función del enunciado
usuariocompartido/P@ssw0rd	usuario para compartir un recurso en otro equipo
invitado	invitado

4. CORTAFUEGOS LOCAL

Cortafuegos local

Elección de un cortafuegos comentando cuales se han valorado.

Configuración segura del cortafuegos elegido comentando los aspectos que hemos tenido en cuenta en la configuración y las modificaciones realizadas a medida que avanza el enunciado.

Modificar la configuración segura del cortafuegos para que todos los equipos respondan al ping: permitan el trafico **ICMP**.

Modificación del cortafuegos para que permita o no compartir un recurso con otros equipos.

Modificación del cortafuegos para que permita o no la administración remota del equipo.

Análisis de vulnerabilidades de nuestro sistema:

Elección de un escáner de vulnerabilidades

Prueba de una herramienta de seguridad que detecte las vulnerabilidades de nuestro sistema.

Justificar todos los puertos abiertos de nuestro sistema explicando porque son necesarios y que programas los utilizan.

5. ANTIVIRUS

Antivirus local

Prueba de varios antivirus gratuitos.

Elección razonada de uno de ellos.

Elección de antivirus para los servidores.

Instalación y configuración adecuada.

Documentar comprobación de funcionamiento correcto: actualizado y activo.

Prueba del antivirus.

Proceso de búsquela de virus en el equipo del equipo.

Establecer y documentar una política de inspección antivirus para la empresa.

Elección, motivación y presupuesto del antivirus elegido para nuestra empresa.

Antivirus on-line recomendados par los usuarios de tu empresa, documenta su funcionamiento.

Discusión y propuesta de otro programas **anti-malware, anti-adware** que has instalado en los clientes de tu empresa.

6. MEMORIAS FLASH Y OTROS DISPOSITIVOS DE INTERCAMBIO DE DATOS

Arranque automático desde un dispositivo conectado al equipo:

Configuración correcta para evitar el arranque automático.

Detección de virus en una memoria flash.

Almacenamiento seguro (cifrado) de la información:

Configuración correcta de seguridad (password o/y cifrado) en el caso de perdida.

Valoración del software que has probado en el cifrado de los datos almacenados en un dispositivo USB.

Deshabilitar puertos y dispositivos de entrada en nuestro equipo:

Configuración segura de otros dispositivos de entrada; anulación de dispositivos para impedir introducir o sacar información a través de ellos.

Borrado seguro:

Localiza y prueba un software de borrado seguro de un dispositivo de almacenamiento.

Recuperación de ficheros borrados:

Localiza y prueba un software de recuperación de documentos borrados de un dispositivo de almacenamiento.

7. OTROS MECANISMOS DE SEGURIDAD

Configuración de la BIOS

Desactivar en el arranque en modo seguro de W7 (F8).

Poner contraseñas en la BIOS y modificar el arranque para que no puedan arrancar desde CD o DVD o USB y cargar una imagen live para la eliminación de contraseñas o el copiado de información del disco de nuestro sistema sin pasar por el control de acceso.

Configuración del inicio de sesión

Evitar que se muestren las cuentas del sistema en el inicio de sesión. El usuario debe conocer el usuario y el password para entrar en el sistema.

Evitar que salga el nombre del último usuario que utilizó el equipo.

Política de gestión de contraseñas de la empresa

Definir la forma y periodo de vigencia de las cuentas del sistema.

Estudia y propón a los empleados de tu empresa un sistema seguro para el almacenamiento de sus contraseñas.

Navegador

Ventajas e inconvenientes de los navegadores en el mercado.

Como elegir un navegador seguro.

Configuración de seguridad de los navegadores de Internet.

Buscadores de Internet.

Administración del historial de navegación.

Localiza un software de control parental para unos padres que quieren controlar la navegación de sus hijos.

Describir otros mecanismos de seguridad que consideras importante y has utilizado explicando características y utilidad.

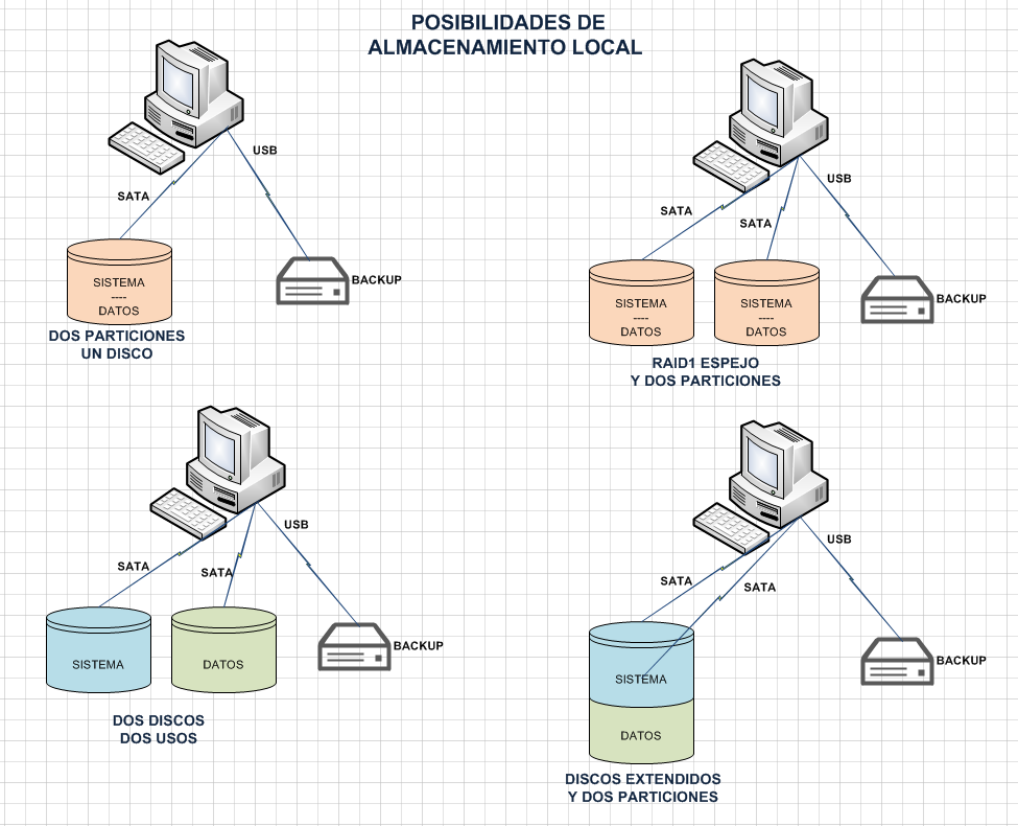
8. PREPARAR SISTEMA DE FICHEROS

Gestión de particiones o discos físicos:

Sería conveniente disponer en la máquina de una unidad de disco para los datos (**DATOS**) separada de la unidad donde está instalado el sistema operativo (**SISTEMA**); es en esta unidad donde crearemos el sistema de ficheros para nuestras pruebas.

Sería conveniente también crear otra unidad para simular un disco duro externo u otro disco duro físico para la realización de las copias de seguridad y almacenar las copias de las imágenes del sistema (**BACKUP**).

Discusión: ¿Donde deben montarse las particiones en linux en los sevidores? (/media/ en los clientes).



Particiones Linux recomendadas (LM51):
Disco1: **/boot** (1GB-Ext4) **/** (95GB-Ext4) **/home** (400GB-Ext4) **linux swap** (4GB-SWAP)
Particiones Linux recomendadas (US12):
Disco1: **/boot** (1GB-Ext4) **/** (95GB-Ext4) **/var** (400GB-Ext4) **linux swap** (4GB-SWAP)
Particiones Windows recomendadas (W750 – DC10):
Disco1: **Arranque** (100MB-NTFS) **Sistema (C:)** (150GB-NTFS) **Datos (D:)** (300GB-NTFS) **Backup (E:)** (50GB-NTFS)
Disco2: 500 GB Disco3: 500 GB

RAID1:

- Windows (DC10): Reflejado Disco2 y Disco3
- Linux (US12): Espejo Disco2 y Disco3.

Gestor de particiones:

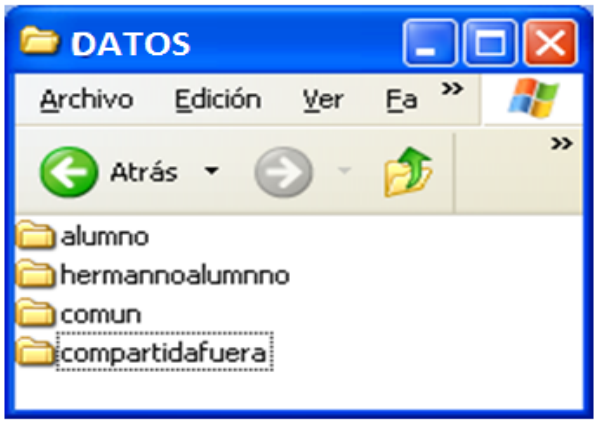
Los equipos cliente de nuestra empresa tienen dos particiones, una de SISTEMA y otra de DATOS.

El servidor de ficheros tiene dos particiones, una de sistema y otra de datos y un disco USB o NAS para almacenar las copias de seguridad (que podemos simular con una partición más: BACKUP).

Documentar el gestor de particiones utilizado.

Ej. Minitool Partition Wizard

Sistema de ficheros en la unidad de DATOS**:**



Rellenar estos directorios con algunos contenidos de ejemplo.

9. CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA DE FICHEROS

El usuario **alumno** tendrá control total sobre los contenidos de las carpetas *alumno*, *comun* y *compartidafuera.*

El usuario **hermanoalumno** tendrá control total sobre su carpeta *hermanoalumno* y solo de lectura y ejecución sobre la carpeta *comun*.

La carpeta *compartidafuera* debe ser accedida con control total por la cuenta **alumno** y por el usuario **usuariocompartido** desde otro equipo conectado en la misma LAN, simulando otro equipo que pudiésemos tener en casa.

Nota Windows:

> ***Panel de control\Redes e Internet\Centro de redes y recursos compartidos\Configuración de uso compartido avanzado***
>
> ***Inicio\Equipo\Administrar\Usuarios y grupos***
>
> ***Inicio\Equipo\Administrar\Carpetas compartidas***
>
> ***No olvidar crear la cuenta en el equipo desde el que nos conectamos al recurso compartido.***

Cuotas de disco:

Estudiar la posibilidad de limitar la cuota de disco de los usuarios de tu empresa.

Nota Linux:

> ***df -h***
>
> ***lsblk -l*** ***lsblk -a*** ***lsblk -fn***

Seguridad de almacenamiento:

Valorar distintos sistemas y configuración del almacenamiento de los datos de tu empresa: particiones, discos, RAID, FreeNAS, SAN, …

Explicar la configuración elegida para el almacenamiento de los datos y de las copias de seguridad de los datos de tu empresa.

10. CREAR UNA CARPETA Y DOCUMENTO CON ACCESO RESTRINGIDO.

Utilidad: proteger la información que tenemos en la unidad de Datos o en la memoria flash para el caso de pérdida o robo.

Formas de restringir el acceso a una carpeta. Documentar y probar.

Formas de restringir el acceso a un documento. Documentar y probar.

Formas de saltarnos esta restricción.

Cifrado y descifrado de documentos.

True Crypt

Rohos

Cifrado simétrico.

Generación de certificados.

Administración de certificados.

Cifrado asimétrico y utilización de certificados digitales.

Resumen o Hash de un fichero

Firma digital.

Encrypting File System (**EFS**) es un sistema de archivos que, trabajando sobre NTFS

11. CONTROL DE ACCESO DE LOS USUARIOS A LAS APLICACIONES.

Utilizando una aplicación concreta (ej paint) hacer que la cuenta **alumno** si que la pueda utilizar pero la cuenta **hermanoalumno** no.

Software instalado en un equipo para un cliente normal con conexión a Internet:

Preparar un protocolo de instalación y configuración inicial de un equipo.

Discusión sobre las instalaciones básicas necesarias en un puesto cliente.

Probar la instalación desatendida de aplicaciones desde la web www.ninite.com

12. CONTROL DE ACCESO DE LOS USUARIOS A INTERNET

Los dos usuarios tienen acceso a Internet, pero *hermanoalumno* solo puede acceder a dos webs:

http://es.wikipedia.org

www.educa.jcyl.es

Describe los mecanismos de seguridad que afectan a la configuración de los navegadores de Internet que utilizas.

Mozilla Firefox en **modo seguro**

Mozilla Firefox R-kiosk **modo kiosco**

> R-kiosk (Real Kiosk) desactiva en Firefox todos los menús, barras de herramientas, comandos de teclado y el botón derecho del mouse y arranca el navegador en pantalla completa como se ve en la imagen. Para acceder a la página de inicio la extensión permite el uso de la combinación Alt+Home. Combinada con una página de inicio que contenga enlaces populares, es una extensión ideal para cibercafés cuyos usuarios deben poder navegar pero no modificar el funcionamiento del navegador. Obviamente, al estar deshabilitadas todas esas características del navegador, para desinstalar la extensión se requiere que se arranque Firefox en modo seguro, algo que debes tener en cuenta si quisieras probarla.

Historial de exploración

Gestión de Password

Navegación privada

Navegación infantil - Control parental

Localiza y prueba algún programa de control parental para tu equipo.

13. COPIA DE SEGURIDAD DEL SISTEMA DE FICHEROS

Estudia y valora distintos programas de copia de seguridad para tu empresa, el resto del ejercicio lo realizamos sobre el software elegido.

De los tres directorios creados.

Describir los procedimientos de copia que has elegido y la forma de realizar la copia.

Definir una política de copia de seguridad para tu empresa.

Copia de seguridad en Internet: proponer un centro de respaldo en Internet para las copias de seguridad de la empresa.

Copia cifrada y comprimida.

Cuenta especial "***operadorcopia/P@ssw0rd***" para la realización y recuperación de copias de seguridad.

Copia automática y desatendida.

Proceso y protocolo de recuperación de una copia (una parte de la copia).

14. RECUPERACIÓN DE UNA COPIA DE SEGURIDAD

Esta actividad debe realizarse con la cuenta "operadocopia"

De todo lo copiado, recuperación de una copia completa.

15. RECUPERACIÓN DE PARTE DE UNA COPIA

Esta actividad debe realizarse con la cuenta "operadocopia"

De un directorio concreto de la estructura copiada.

Debemos tener definido el proceso de recuperación de un documento de las copias de seguridad y donde le dejamos la información solicitada al usuario que nos lo ha pedido.

Debemos comprobar que el usuario que ha solicitado la información de la copia tiene acceso al documento que le hemos recuperado.

16. IMAGEN DEL SISTEMA

Valorar distintas formas de hacer la imagen, explicar el proceso de realización.

Clonezilla

Punto de restauración de Windows

Ventajas e inconvenientes de las dos estrategias anteriores.

Almacenamiento de las imágenes del sistema: **servidor de imágenes** del sistema (utilizando la máquina US12).

Puntos de restauración del sistema

Estudiar, documentar y probar los puntos de restauración.

Copia del registro

Imagen del sistema

Sysprep

Virtualización

Virtual Box

Proxmox

Congelación

Thin client – cliente ligero

17. EQUIPO CON VARIOS SISTEMAS – GESTOR DE ARRANQUE

Valorar distintos gestores de arranque: ventajas, inconvenientes, características.

Protección del gestor de arranque para impedir su manipulación y el arranque desde un sistema no autorizado (live).

Elegir uno y crear una máquina virtual con dos sistemas. Describir el proceso.

Procedimiento para copiar una partición con un sistema instalado en otra que esté vacía (esto nos permitiría tener una copia de una imagen para reemplazar otra si se deteriorase).

Software de recuperación automática del sistema.

18. EQUIPO CON VARIOS SISTEMAS Y UN ESPACIO EN DISCO COMPARTIDO

Queremos tener una unidad de disco (virtual) con el sistema de ficheros descrito accesible por los dos sistemas.

La configuración óptima de este ejercicio sería:

Partición con sistema operativo **Windows** 7 y el software instalado en este sistema.

Partición con sistema operativo **Linux** y el software instalado en este sistema.

Partición de **datos**.

Partición de **backup** y copia de imágenes.

19. MANTENIMIENTO DE SISTEMAS ESPECÍFICOS

Instalación de actualizaciones

Corregir fallos detectados – (en muchos casos mejorar la seguridad)

Añadir nuevas funcionalidades

Servidor de imágenes del sistema.

Servidor de virtualización.

Utilización segura en entornos vulnerables

Evitar el reenvío de mensajes masivos de correo electrónico (spam, phising).

Uso de la copia oculta.

Utilizar contraseñas fuertes en redes sociales.

Tener precaución en las formas de pago en las compras de Internet.

Estudio sobre las formas de pago

PayPal

Equipo estable

Seguridad aplicada a un equipo utilizado por muchos usuarios que no pueden guardar nada ni modificar la configuración del equipo (cibercafé, biblioteca, aula de informática,…). Definir el procedimiento que sigue el administrador para modificar la configuración de estos equipos.

Punto de información

Seguridad aplicada a un equipo que presenta al usuario únicamente un navegador web (punto de información): punto de información del ayuntamiento, Renfe,… Definir el procedimiento que sigue el administrador para modificar la configuración de estos equipos.

Mantenimiento de un conjunto de equipos iguales (hardware y funcionalidad).

Estrategia de seguridad para el mantenimiento de un aula de informática con 15 equipos iguales, teniendo en cuenta que los usuarios de los equipos pueden realizar modificaciones sobre su configuración, guardar información en ellos… pero estas modificaciones no deben mantenerse cuando finaliza el curso. Definir el procedimiento que realiza el administrador para restaurar o modificar la configuración de estos equipos.

Servidor de terminales

Estrategia de seguridad para un aula con un servidor (ej. edubuntu) y clientes que corren terminales que se ejecutan en el servidor.

Servidor de virtualización

Estrategia de seguridad para un aula con un servidor (ej. edubuntu) y clientes que corren máquinas virtuales que se ejecutan en el servidor.

Congelación del sistema

Estrategia de seguridad para un equipo con (parte de) el sistema congelado.

Monitorización remota de todos los equipos de un aula

iTalc

Administración remota

-----**FIN EXAMEN PRÁCTICO 1**----------

EXAMEN PRÁCTICO 2: SEGURIDAD EN EL SERVIDOR Y EN LA LAN - DETALLE

OBJETIVO:

El objetivo del ejercicio es la puesta en práctica de aspectos relacionados con la seguridad informática en una LAN de una pequeña empresa con equipos de usuario, servidores dedicados; con distintos sistemas operativos y usuarios con distintos privilegios.

PUNTO DE PARTIDA

Maquina virtual Oracle Virtual Box

- Windows 7 / Windows X
- Linux Desktop
- Windows 2012 server
- Linux Ubuntu Server (con los servicios mínimos necesarios)

NOTA: desactivamos las actualizaciones automáticos de Windows para que la máquina virtual consuma menos recursos; en condiciones normales deberían estar activadas.

NOTA2: quien lo desee puede sustituir los sistemas operativos recomendados por otros, previa consulta al profesor.

NOTA3: al finalizar el ejercicio el alumno deberá entregar la documentación del trabajo realizado y las máquinas virtuales que el profesor estime oportuno.

NOTA4: en la medida de lo posible realizaremos el ejercicio también sobre máquinas reales.

20. INSTALACIÓN Y CONFIGURACIÓN INICIAL DE LA RED DE ÁREA LOCAL DE LA EMPRESA. DOCUMENTACIÓN Y DESCRIPCIÓN DE LA CONFIGURACIÓN DE LA EMPRESA.

Instalación de Windows Server 2012, Windows 7 y Linux Desktop en los equipos que sea necesario.

Instalación

Identificación

Configuración de red

Configuración segura de antivirus y cortafuegos

Prueba de conectividad

Características técnicas de los equipos utilizados.

Realizar un modelo de red de la empresa.

Crear una base de datos con los equipos disponibles en la empresa.

- Identificador
- Modelo de placa
- Procesador
- RAM
- Disco duro
- CD/DVD…
- Tarjetas de red / MAC /IP
- Utilidad en la empresa
- Descripción…

Nombre de dominio: `xxxxxxxxxx.local`

Cuenta de administración de los equipos:

administrador / P@ssw0rd **miadmin/P@sw0rd**

Crear una cuenta auxiliar de administrador de reserva.

miadmin2 / P@ssw0rd

Asignar nombres correctamente a los equipos de la empresa.

Realizar una ficha de cada equipo donde recogemos las características del equipo y los procesos (clientes o servidores) que vamos instalando en él.

Colocar esta ficha como fondo del escritorio en el equipo al que corresponde.

Colocar en el escritorio accesos directos a las herramientas administrativas de los servicios instalados en cada equipo.

Mantener el escritorio ordenado.

Configuración de las direcciones IP de la empresa. IP´s estáticas.

Realizar y mantener actualizada la tabla:

Equipo / Sistema operativo/ Disco-Particiones /RAM / Tarjeta de red MAC -configuración IP...

21. CONFIGURACIÓN DE LA ADMINISTRACIÓN REMOTA SEGURA DE LOS EQUIPOS DE LA EMPRESA.

Los servidores solo pueden ser administrados de forma remota desde la máquina W750 que es el equipo del administrador de red.

Utilizar conexiones seguras (SSH) para la administración remota.

Configurar los cortafuegos locales y de red para que los equipos no puedan ser administrados de forma remota desde cualquier sitio.

Restringir la administración remota desde fuera de la LAN. Autorizarla solo en caso necesario para personas concretas. En condiciones normales no se permite la administración remota de los servidores desde Internet.

Utilización de certificados para las cuentas autorizadas a realizar la administración remota.

Utilización de VPN para accesos remotos desde Internet.

Herramientas recomendadas:

Windows: **Conexión a escritorio remoto**.
Teamviewerhost
Linux: **Notepad++**, **Putty**.

Usuarios con administración remota

Administrador, admin, operadorcopia, operadordominio.
El resto de usuarios no tienen administración remota.

Ubicación de los equipos cliente de administración remota

Administración remota desde la LAN: el cliente y el servidor están en la misma red.
Administración remota desde Internet: el cliente y el servidor están en redes distintas.
Administración remota desde Internet utilizando un servidor intermedio; normalmente un servidor https (ej, teamviewer, joinme,…)

Instalación del teamviewerhost en la máquina dc10.

Administración remota de máquinas Windosws 2012 Server.

Conexión remota.
Monitorización del sistema.
Instalación y configuración de servicios. Utilización de las consolas administrativas personalizadas o las predeterminadas de los servicios instalados.
Gestión de ficheros de log.
Tareas y scripts de administración.
Administración de actualizaciones.
Instalación de software.
Copia de seguridad y recuperación de configuraciones.
Copia de seguridad y recuperación de datos.

Administración remota de servidores Ubuntu Server.

Conexión remota.
Monitorización del sistema.
Instalación y configuración de servicios.
Gestión de ficheros de log.
Tareas y scripts de administración.
Administración de actualizaciones.

Administración remota de máquinas Cliente.

Conexión remota. Asistencia on-line para solución de problemas.
Instalación desatendida.
Administración de actualizaciones.

Administración remota del servidor de virtualización

Creación de máquinas virtuales.
Parametrización, clonación, eliminación, ajuste,… de las máquinas virtuales.
Administración y monitorización del servidor de virtualización.

22. INSTALACIÓN Y CONFIGURACIÓN SERVIDOR DNS DE LA EMPRESA.

Activar el servidor DNS interno de la empresa.

Elegir un nombre para el dominio de la ***empresa*.local**

Activar el servidor DNS y comprobar su correcto funcionamiento.

Zona directa / Zona inversa
Servidor primario / Sevidor secundario
Sugerencias de raiz
Reenviadores
Actualización automática de nuevos registros para cuando nuestro servidor forme parte de un dominio de active directory.

Clientes DNS

Configuramos todos los equipos de nuestra empresa para que sean clientes de nuestro servidor DNS.

Configuración del sufijo DNS correcto de todos los clientes de la empresa (ojo que los servidores linux son clientes DNS).

Prueba de la resolución de nombres desde todos los clientes.

Administración y monitorización del servidor DNS.

Copia de seguridad de la estructura DNS

Restauración de una copia de seguridad de la estructura DNS

Activar el servidor DNS público de la empresa.

Instalación y configuración del simulador de dominio raíz de Internet.

.es

Instalación y configuración del dominio público de la empresa.

empresa.es

23. INSTALACIÓN Y CONFIGURACIÓN DEL CONTROLADOR DE DOMINIO - SERVIDOR AD DE LA EMPRESA.

Activar el servidor AD de la empresa.

Crear un controlador de dominio de **Active Directory / LDAP (openLDAP)**; Uso y disfrute de la herramienta administrativa correspondiente para cuentas de usuarios, equipos, directivas de seguridad de todos los sistemas de la empresa.

Administración y monitorización del controlador de dominio.

Añadir los cliente Windows al controlador de dominio de la empresa.

Añadir los clientes Ubuntu al controlador de dominio de la empresa.

Copia de seguridad y restauración de la estructura Active Directory / LDAP (openLDAP)

Instalación en la empresa de un controlador de dominio secundario para sustituir al primario en caso de fallo

Trasladar a esta máquina ***otros servicios replicados*** para mejorar la disponibilidad del servicio (DNS, DHCP, servidor de ficheros, impresión…)

24. INSTALACIÓN Y CONFIGURACIÓN SERVIDOR DHCP DE LA EMPRESA.

Activar el servidor DHCP de la empresa. IP´s dinámicas.

Instalar y configurar un servidor DHCP para LAN de la empresa.

Activar el servidor DHCP comprobar su correcto funcionamiento.

Modificar los clientes para una configuración IP dinámica.

Comprobar el correcto funcionamiento del servidor DHCP con diferentes configuraciones:

Rango de direcciones.
Reservas por MAC.
Exclusión de direcciones.
Periodo de concesión.
Información enviada al cliente.

Administración y monitorización del servidor DHCP

Copia de seguridad y restauración de la estructura DHCP

Control de la clientela del servidor

Puesto que en clase, todos los equipos correspondientes a las empresas están conectados con el mismo switch, los servidores DHCP que se activen lo estarán para todas las empresas, en el mismo segmento de difusión. (Si nuestras máquinas están todas en el mismo equipo anfitrión, podemos evitar este problema poniendo la configuración de red de las máquinas virtuales en "red interna" mientras probamos el servicio DHCP)

Debemos tener esto en cuenta a la hora de probar el correcto funcionamiento de nuestro servidor DHCP.

Lo correcto que el servidor DHCP reparta un numero de direcciones mínimo y con reserva de MAC para las máquinas de nuestra empresa.

Alta disponibilidad DHCP (utilizando la máquina DC11)

Alternativas:

- Agente de retransmisión de DHCP (proxy DHCP)
- DHCP Fileover (Redundancia DHCP) a partir de Windows 2012.
- Redundancia con rangos disjuntos.

25. ADMINISTRACIÓN DEL DOMINIO.

Cuentas de usuario de la empresa:

Recursos compartidos y restringidos para la empresa:

Directivas de seguridad y control de recursos en Windows 2012 Server:

(Utilizando Active Directory / LDAP y el dominio correspondiente)

Las empresas deberán disponer de las siguientes **cuentas normales de usuario / password** (que podrán utilizarse en cualquier equipo cliente de la empresa):

jefe1 / P@ssw0rd

jefe2 / P@ssw0rd

currito1 /P@ssw0rd

currito2 /P@ssw0rd

Otras cuentas administrativas del dominio:

administrador / P@ssw0rd: Cuenta de administrador del dominio.

miadmin2 / P@ssw0rd: Cuenta de administrador del dominio de reserva.

operadordominio / P@ssw0rd: Cuenta que utilizaremos solamente para meter y sacar equipos del dominio.

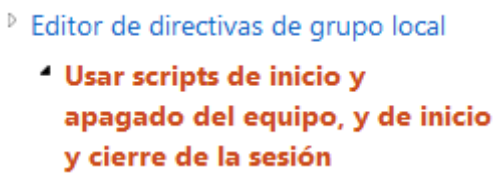
operadorcopia / P@ssw0rd: Cuenta con permisos para realizar y restaurar las copias de seguridad.

Solo las cuentas *administrador* y *admin* tendrán permiso de ***inicio de sesión local*** en el servidor.

Todas las cuentas administrativas (*administrador*, *admin*, *operadorcopia*, *operadordominio*) tendrán permiso de ***administración remota*** sobre el servidor Windows. Solo las cuentas administrativas podrán realizar la administración remota del servidor.

Definir una política de contraseñas correcta para una empresa real.

Editor de directivas de grupo local



Estructura de almacenamiento del servidor de ficheros

El controlador de dominio dispone de tres particiones o discos: **Sistema, Datos y Backup**.

Sobre la unidad **Datos**:

La empresa dispondrá de un **servidor de ficheros** (w2012Server) ubicado en el controlador de dominio con la siguiente estructura de directorios:

/DatosEmpresa	**/jefe1/**	
	/jefe2/	
	...	
	/currito1/	
	/currito2/	
	…	
	/Administrador/	
	/miadmin2/	
	/operadorcopia/	
	/operadordominio/	
	...	
	/ComunJefes	
	/ComunCurritos	
	/DocumentosRecuperados/	
	/BandejaImpresora/	
/Administración	**/Scripts/**	(sysvol ??)
	/CopiasConfiguracion/	
	/Software/	
	/Administrador/	
	/miadmin2/	
	/operadorcopia/	
	/operadordominio/	
	...	

Acceso al servidor de ficheros:

Los jefes tendrán **acceso total** a su ***directoriopersonal*** de cuenta y al directorio ***ComunJefes*** y al directorio ***ComunCurritos***.

Los curritos tendrán **acceso total** a su ***directoriopersonal*** de cuenta y al directorio ***ComunCurritos***.

Todas las cuentas tendrán acceso a la ***BandejaImpresora*** y al directorio ***DocumentosRecuperados***.

En principio, Jefes y Curritos **no tendrán acceso a más información en el servidor**.

Establecer la política adecuada de **permisos** y **recursos compartidos** para cumplir con las especificaciones del enunciado.

Conexión automática al servidor de ficheros:

Cuando se conectan a un equipo desde un puesto cliente:

todas las cuentas deben tener asociada una unidad **Z:** a su directorio de trabajo en el servidor de ficheros

todos los jefes una unidad **Y:** al directorio del grupo (*/ComunJefes/*

todos los jejes y todos los curritos **X:** asociada al directorio */ComunCurritos/*.

Cuando pongamos en marcha el servicio de impresión y el procedimiento de copia de seguridad serán necesarias dos unidades más para todas las cuentas:

W: asociada al directorio */BandejaImpresion/*

V: *asociada al directorio /DocumentosRecuperados/*

Crear los scripts de conexión **InicioJefes.bat**, **InicioCurritos.bat** y colocarlos en sysvol y asignar estos scrips al usuario.

Opción2: Mapear las unidades utilizando las GPO. (Forzar la actualización de directivas en el cliente con gpupdate /force)

Creación rápida de nuevas cuentas de usuario:

Crear dos (uno para cuentas "currito" y otro para cuentas "jefe") ficheros batch que, solicitando como parámetro el nombre de la cuenta (ej.: "currito10" o "jefe20"), cree la estructura de ficheros necesaria y la cuenta correspondiente con todas las características de una cuenta "currito" o "jefe".

Control de horario de conexión y equipos que pueden utilizar los usuarios:

Los curritos únicamente podrán conectarse desde los puestos cliente (donde tenemos Windows 7) y en su horario de trabajo.

Los jefes podrán conectarse desde cualquier equipo y a cualquier hora, incluido el servidor.

Perfiles de conexión:

Los Jefes dispondrán de un perfil móvil con un acceso directo a LibreOffice Writer en el escritorio.

Los curritos dispondrán de un perfil obligatorio con un acceso directo a LibreOffice Calc en el escritorio.

Control de conexiones simultaneas: (Limitlogon.exe)

Los jefes podrán establecer hasta dos conexiones simultáneamente en dos equipos distintos.

Los curritos únicamente podrán tener una conexión abierta.

Los administradores y operadores solo podrán tener una conexión abierta.

Lanzar programas en el establecimiento de conexión.

Cuando se conecta un currito, el LibreOffice Writer (del equipo en el que se conecta) se abre automáticamente. Suponemos que todos los equipos tienen instalado el LibreOffice en el mismo sitio.

Monitorización de conexiones

Windows:

- Inicio / cierre de sesión
- Conexión fallida
- Control de acceso a un recurso

Linux:

- /var/log/auth.log
- /var/log/secure

Copia de seguridad y recuperación de la estructura AD / LDAP

Alta disponibilidad

Dominio secundario

DFS

Alta disponibilidad LDAP

Nota: probar la herramienta de Windows **psr.exe** para la documentación de un trabajo concreto sobre el servidor.

26. INSTALACIÓN Y CONFIGURACIÓN DEL SERVICIO DE BACKUP.

Servicio de backup sobre el controlador de dominio

Discusión sobre el software de copia mas adecuado para nuestra empresa.

Administración y monitorización del servidor de copia.

Datos comprimidos y cifrados en la copia de seguridad.

Política de copia de seguridad de la empresa.

Realización de una copia.

Recuperación de una copia total.

Recuperación de una copia parcial.

Servidor de imágenes del sistema

Discusión sobre el software mas adecuado para realizar las imágenes.

Imagen de disco, imagen de partición.

Administración y monitorización del servidor de imágenes del sistema.

Política de gestión de imágenes de los sistemas de la empresa.

Sysprep de Microsoft.

Realización de una imagen.

Recuperación de una imagen.

Copias de seguridad de la configuración de servicios específicos

Utilizar el directorio */Administracion/CopiasConfiguracion/* para guardar estas copias.

Exportar / **Importar** la configuración de los servicios: DNS, AD, LDAP, DHCP, …

Utilizar scp (ssh) para mover los ficheros de configuración de linux.

27. INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR DE IMPRESIÓN PARA LA LAN DE LA EMPRESA.

Instalar un servidor de impresión.

Utilizaremos una impresora virtual (pdfcreator) que deberá dejar los documentos en el directorio /DatosEmpresa/BandejaImpresion/ accesible a todas las cuentas del sistema.

Instalar la impresora
Compartir la impresora
Configurar los clientes del servicio de impresión, utilizar un script de inicio de sesión para conectar la impresora en los clientes.

Log y registro de documentos enviados a la impresora por los usuarios de la empresa.

Envío al correo electrónico del usuario del documento escaneado en la impresora.

Instalación de una impresora de red asociada al servicio de impresión.

Compartir una impresora local para que pueda ser utilizada por otro equipo de la misma LAN.

28. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR WEB PARA LA INTRANET DE LA EMPRESA.

Apache o IIS

Sobre Windows 2012

Sobre Ubuntu Server

Configuración del servidor DNS para que los clientes puedan acceder fácilmente a la información de la intranet de la empresa. (www.empresa.local)

Copia de seguridad que permita recuperar un servidor web de un desastre

HTTPS

Convertir nuestro servicio web en un servicio seguro utilizando el protocolo HTTPS.

Documentar la generación del certificado necesario para montar nuestro servidor HTTPS.

Utilizar una Autoridad de Certificación propia (de nuestra empresa) para la generación del certificado e instalarlo en el servidor HTTPS.

Webdav: extensión de HTTPS para utilizar el servidor web como servidor de ficheros.

Virtualización de dominios

Instalación y configuración de un servidor web para el dominio público de la empresa

Administración remota del servidor web:

Administración remota del espacio web: Abrimos el puerto 22 para la administración remota del espacio web asignado a cada cliente.

Usuarios ejaulados con SFTP: para que no manipulen el servidor fuera de su carpeta de trabajo. (Estas cuentas no pueden iniciar sesión desde el Putty)

DMZ – Ofrecer un servicio web en Internet

Creación de una DMZ en la LAN de la empresa donde poder ofrecer un servicio de alojamiento web a usuarios de Internet:

Redirección de puertos en el firewall que permita y controle el acceso de los usuarios a los servicios que ofrece en Internet.

Política de DNS

Gestión de acceso para el mantenimiento del alojamiento contratado

Organización del servidor, estructura de almacenamiento, paquetes de software, balanceo de utilización de la conexión a Internet.

Seguridad y alta disponibilidad de nuestro servicio web

29. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR FTP / SFTP.

Conectado a la estructura de ficheros de la intranet de la empresa

Sobre W2012 Server, Ubuntu Server

Instalación y configuración inicial del servidor FTP / FTPS / SFTP / SSH

Elección de un cliente FTP para instalarlo en todos los equipos de la empresa.

Manual de utilización del cliente FTP: configuración y uso.

FTP - File Transfer Protocol

http://es.wikipedia.org/wiki/File_Transfer_Protocol

FTPS - FTP/SSL - FTP sobre SSL

http://es.wikipedia.org/wiki/FTPS

SFTP - SSH File Transfer Protocol

http://es.wikipedia.org/wiki/SSH_File_Transfer_Protocol

Conexión segura con el servicio SFTP. Nos aseguramos de que movemos la información de formas segura.

Documentar la utilización del comando **sftp**.

SSH - Secure Shell

http://es.wikipedia.org/wiki/Secure_Shell

Alternativa para mover ficheros de forma segura utilizando el comando **scp**.

Utilidades de los servidores FTP / SFTP

Mantenimiento de los contenidos de los servidores web. Conectado a la estructura de ficheros de la web pública o intranet de la empresa.

Utilización del servidor FTP para la creación y distribución de imágenes del sistema.

Utilizado para realizar copias de seguridad remotas.

Log remotos.

En general, para mover de forma segura (SFTP / SSH) ficheros entre dos máquinas.

30. REDUNDANCIA Y ALTA DISPONIBILIDAD

Redundancia fisica de discos y otros componentes hadware.

Discos RAID
Fuente de alimentación
Tarjetas de red
CPD redundante
Generadores eléctricos

Instalación en la empresa de un controlador de dominio secundario para sustituir al primario en caso de fallo

Trasladar a esta máquina otros servicios replicados para mejorar la disponibilidad del servicio (DNS, DHCP, servidor de ficheros, impresión…)

Servidos DNS secundario

Servidor DHCP Secundario

Servidor de ficheros secundario - DFS

Servidor de impresión secundario

Alta disponibilidad en la conexión a Internet de la empresa – Balanceo de carga

Alta disponibilidad en los switch de la LAN, en la conexión a la red de los servidores

Pruebas de la configuración de alta disponibilidad

Entrenamiento de las situaciones de desastre y detalle de los protocolos de actuación.

-----**FIN EXAMEN PRÁCTICO 2**----------

EXAMEN PRÁCTICO 3: SEGURIDAD EN LA CONEXIÓN A INTERNET - DETALLE

OBJETIVO:

El objetivo del ejercicio es la puesta en práctica de aspectos relacionados con la seguridad informática en la conexión a Internet de la empresa.

31. INSTALACIÓN Y CONFIGURACIÓN EN LA EMPRESA DE UNA RED INALÁMBRICA, AMPLIANDO LA LAN.

Añadir a la empresa un nuevo equipo cliente utilizando una red inalámbrica (PCI o USB).

Conectar a la LAN de la empresa la base inalámbrica.

Configuración de la base inalámbrica.

Instalación de tarjetas de red USB y PCI inalámbricas.

Configuración de la tarjeta de cliente inalámbrico.

Aseguramiento de la red inalámbrica.

Proponer y desarrollar una configuración segura de la red wifi de la empresa.

Crear una DMZ para ofrecer el servicio wifi en la empresa.

Aseguramiento de la red inalámbrica.

Desarrollo de un **portal cautivo** para ofrecer servicio wifi en la empresa.

Instalación y configuración de un servidor RADIUS (**FreeRADIUS**)

Documentar la infraestructura (alternativas), proceso de configuración y proceso de administración de los usuarios del portal cautivo (altas, modificaciones, bajas, informes de uso)

Ataque a la red inalámbrica de otra empresa.

Realizar un ataque a la red wifi de un compañero.

32. INSTALACIÓN Y CONFIGURACIÓN DEL ROUTER QUE DA SALIDA A INTERNET EN LA EMPRESA.

Enrutamiento estático:

Documentar la tabla de rutas utilizada.

Enrutamiento dinámico: RIP v1, RIP v2, OSPF, OSPF + RIP

Enrutamiento sobre:

W7
W2012Server
Ubuntu Server
Router Wifi
Router Cisco, …

Traducción de direcciones y puertos: NAT – PAT

Ocultar direcciones privadas y estructura de la LAN en Internet.

Redirección de puertos necesaria para el correcto funcionamiento de los servicios ofrecidos en nuestra empresa:

Servicio HTTPS / HTTP
Servicio VPN
Servicio SSH / SFTP
Servicio FTPS / FTP …

Administración y monitorización del servicio de enrutamiento.

Balanceo de carga en la salida a Internet

Instalación de ADSL comunitaria

Estudiar y discutir una instalación de ADSL comunitaria, compartida por una comunidad de vecinos.

Requisitos hardware, software y legales para su implantación.

Presupuesto de instalación y administración.

Problemas de seguridad y responsabilidad en este tipo de instalaciones.

33. INSTALACIÓN DE UN CORTAFUEGOS SOBRE EL ROUTER LINUX.

IPTABLES

Configuración del cortafuegos para implementar **NAT**.

Proponer una configuración segura del **cortafuegos** para la protección de los equipos de la empresa.

Cortafuegos de red en la máquina US01:

LimpiarReglas.sh
MostrarReglas.sh
CortafuegosUS01.sh

Cortafuegos local de la máquina US12:

INPUT: (ejemplo)

Puertos: 22 (ssh), 80 (http), 443 (https) abiertos desde cualquier origen
Todos los puertos abiertos desde las máquinas 50 y 51 para la adm. remota
Conexiones establecidas y relativas permitidas
Resto DROP

DMZ

Proponer una configuración de **DMZ** que nos permita ofrecer servicios en Internet (un servidor web)

Describir el modelo de servidores y servicios que instalaríamos en la DMZ junto con la configuración de los cortafuegos que la componen.

Ejemplo: Abrimos los puertos 80, 443 y 22 y los redirigimos a la máquina US12 para ofrecer estos servicios en Internet.

VPN

(en el servidor VPN)

Configuración del servidor VPN

Discusión sobre la ubicación en la LAN de la empresa del servidor VPN.

Redirección de puertos en el cortafuegos para acceder a él cuando no está situado en el router.

Configuración de los cortafuegos de la empresa para permitir el trabajo desde su casa de forma segura a los “jefes” de nuestra empresa. Configuración del cliente VPN.

Configuración de los cortafuegos de la empresa para permitir la conexión estable y permanente de una sucursal de la empresa en la que los dispositivos deben utilizar los servidores de la sede central de la empresa. Configuración de un túnel VPN permanente entre el router de la sucursal y el de la sede central.

(en el servidor VPN)

Discusión de los problemas de seguridad asociados a las conexiones VPN.

Utilización de certificados en el establecimiento de conexiones VPN.

34. INSTALACIÓN DE UN PROXY WEB SOBRE EL SERVIDOR LINUX.

SQUID

Configurar el proxy web de la empresa, para controlar la navegación de los curritos y permitir una navegación libre a los jefes.

Definir la política de permisos de navegación de los usuarios de la empresa.

Estudiar la posibilidad de los usuarios de saltársela.

Estudiar y dimensionar correctamente los log y la caché del proxy.

Entornos gráficos de configuración y mantenimiento del proxy

Zentyal

Saltarse el proxy

Estudiar las formas de saltarse el proxy que tienen los curritos de tu empresa.

Soluciones.

Consecuencias de saltarse el proxy.

Estudiar y proponer otras alternativas de software o configuración del proxy

WAF

MOD SECURITY

35. INCORPORACIÓN DE UN CLIENTE REMOTO A LA LAN DE LA EMPRESA DESDE INTERNET UTILIZANDO VPN.

Servidor VPN

Configuración del servidor VPN

Discusión sobre la ubicación en la LAN de la empresa del servidor VPN.

(en el router)

Redirección de puertos en el cortafuegos para acceder a él cuando no está situado en el router.

Configuración de los cortafuegos de la empresa para permitir el trabajo desde su casa de forma segura a los "jefes" de nuestra empresa. Configuración del cliente VPN.

Configuración de los cortafuegos de la empresa para permitir la conexión estable y permanente de una sucursal de la empresa en la que los dispositivos deben utilizar los servidores de la sede central de la empresa. Configuración de un túnel VPN permanente entre el router de la sucursal y el de la sede central.

Discusión de los problemas de seguridad asociados a las conexiones VPN.

Utilización de certificados en el establecimiento de conexiones VPN.

VPN de acceso remoto: Configuración de clientes remotos:

Configuración de un cliente remoto que permita a los jefes trabajar desde casa sobre la LAN de la empresa.

VPN punto a punto: Interconexión segura de distintas sedes de una empresa a través de Internet:

Configuración de túneles permanentes para interconectar sucursales de la empresa.

Además de una conexión segura entre sucursales y la sede central, proponer una política de distribución de los servicios (ad, dns,...)

36. AUTORIDAD DE CERTIFICACIÓN

Creación de una **Autoridad de Certificación** propia para los usuarios de la empresa y los servicios que requieran el uso de un certificado.

Emisión de certificados para cada uno de ellos:

Usuarios que requieran un certificado: jefe1, jefe2

Servicios (servidores y clientes) que requieran un certificado: ssh, https, sftp,..

Gestión de **Certificados Digitales**:

Emitir
Revocar
Eliminar
Distribuir

37. UTILIZACIÓN DE CERTIFICADOS

Distribución e instalación de un certificado digital.

Administración de las claves privadas.

Administración y verificación de las claves públicas.

Modificar nuestros clientes para que reconozcan nuestra Autoridad de Certificación como buena.

Utilización de certificados digitales para:

Cifrar un documento / Descifrar un documento.

Firmar un documento. / Comprobar la firma de un documento.

Firmar y cifrar un documento / Descifrar y comprobar la firma de un documento.

SSH / SFTP Autorizar una conexión remota.

HTTPS

FTPS

Correo seguro

...

38. INSTALACIÓN Y CONFIGURACIÓN DE OTROS SERVICIOS DE RED.

PKI

RADIUS

PKI, Active Directory, RADIUS

KERBEROS

LDAP

Servicios de correo electrónico: SMTP, POP3, IMAP. Correo seguro.

Mensajería instantánea. News. Listas de distribución.

Moodle. Joomla.

Windows Media Server.

Voz IP.

…

39. SUGERENCIAS PARA MEJORAR ESTE EJERCICIO

Aspectos de la seguridad del sistema que consideras interesantes y quedan fuera de este enunciado.

40. DOCUMENTACIÓN DEL EJERCICIO.

-----**FIN EXAMEN PRÁCTICO 3**----------

ÍNDICE DE CONTENIDO