Seguridad Informática

IES Los Sauces – Sistemas Microinformáticos y redes

HBM

Distribución temporal

Objetivo de las prácticas de seguridad informática durante el curso.

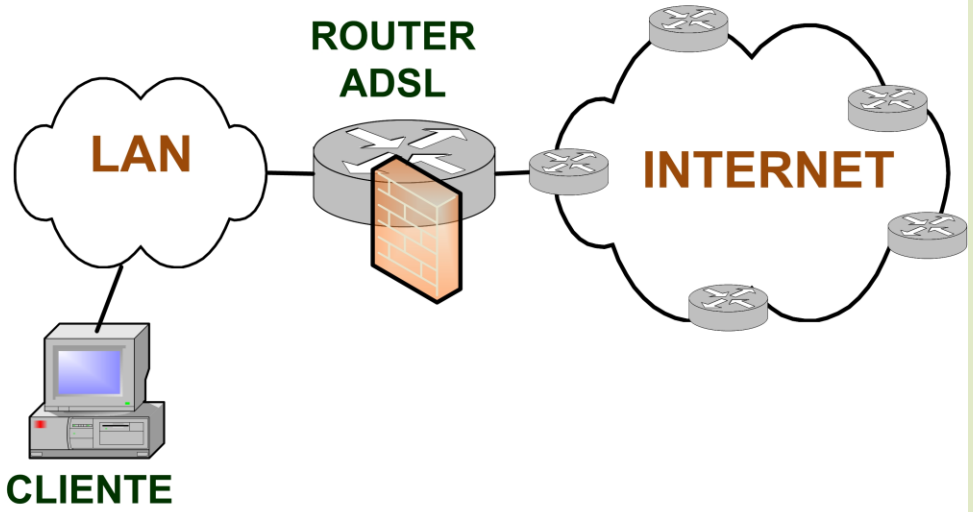
- **Octubre – Noviembre**: **Proteger un equipo cliente**. Técnicas y herramientas de seguridad para proteger un equipo cliente.
- **Diciembre – Enero**: **Proteger un servidor**. Técnicas y herramientas de seguridad para proteger un equipo servidor.
- **Febrero – Marzo**: **Proteger la red de la empresa – LAN**. Técnicas y herramientas de seguridad para proteger la red de la empresa.

Seguridad en la red de un hogar

Planteamiento de seguridad
MODELO GENÉRICO DE LA RED UN HOGAR
Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso**: Usuarios y Grupos locales – S. Activa
  - Seguridad BIOS, arranque
  - Separar cuentas administrador y cuentas de usuario
  - Control de permisos y recursos compartidos.
  - Cifrado de las comunicaciones: SSH, HTTPS,..
  - Cifrado de la información almacenada
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
  - Cortafuegos Local
  - Cortafuegos de Red: en el router ADSL
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos en un soporte externo
  - Partición de datos y sistema (programas) separadas
  - Imagen del sistema o punto de restauración
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
  - Quien puede acceder a nuestro equipo

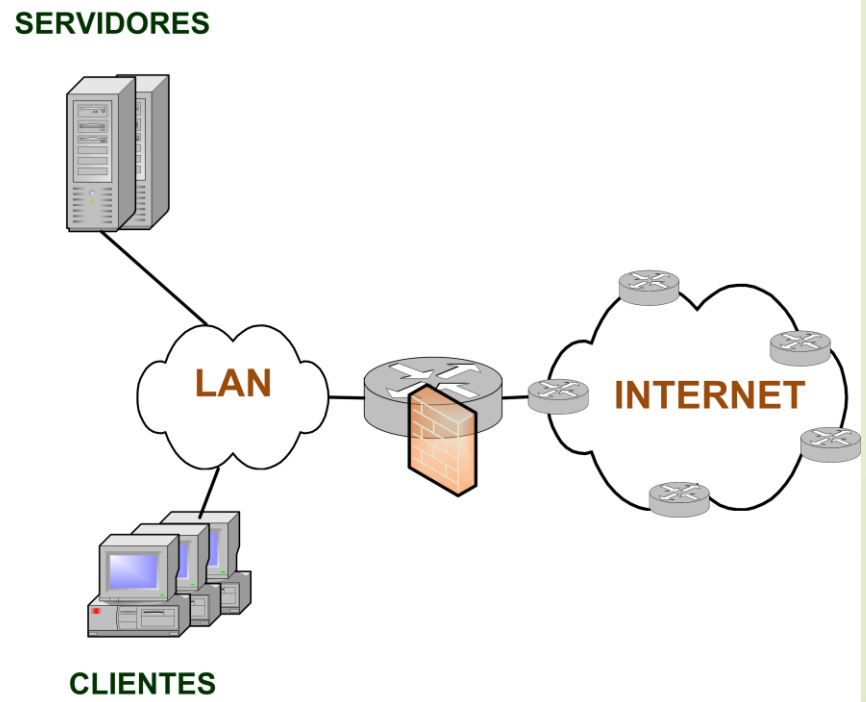
- **Monitorización, Vigilancia** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva



Seguridad en la red de una empresa

Planteamiento de seguridad
MODELO GENÉRICO DE LA RED DE UNA EMPRESA
Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso**: AD, LDAP, SAMBA – S. Activa
  - Seguridad BIOS, arranque
  - Control de acceso centralizado: AD, LDAP, SAMBA
  - Control de permisos y recursos compartidos.
  - Cifrado de las comunicaciones: SSH, HTTPS,..
  - Cifrado de la información almacenada
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
  - Cortafuegos Local
  - Cortafuegos de Red: inspección de paquetes, proxy
  - DMZ (si la empresa ofrece servicios en Internet)
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos del servidor de ficheros.
  - Copia de seguridad de los ficheros de configuración de máquinas y servicios.
  - Imagen del sistema para los equipos cliente
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
  - Quien puede acceder a los servidores
  - Teletrabajo – VPN
  - Sucursales de la empresa
- **Hardware redundante** – Seguridad Pasiva
  - RAID
  - CPD de respaldo
  - Línea de comunicaciones redundante
  - SAI en los servidores
- **Monitorización, Vigilancia, Auditoría** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva



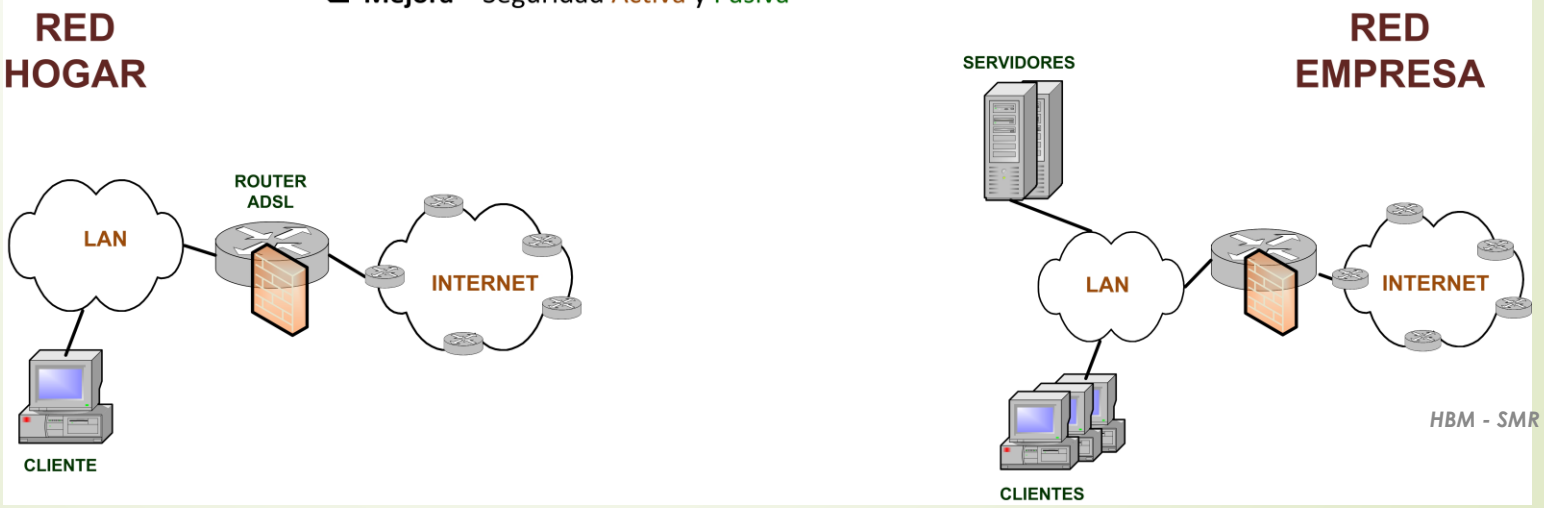
Planteamiento general de seguridad

Planteamiento de seguridad

Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso:** Usuarios, grupos, permisos – Seguridad Activa
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos del servidor de ficheros.
  - Copia de seguridad de los ficheros de configuración.
  - Imagen del sistema para los equipos cliente, puntos de restauración
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
- **Hardware redundante** – Seguridad Pasiva

- **Monitorización, Vigilancia, Auditoría** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva



Equipos **cliente** con conexión a Internet

- Equipo utilizado en un hogar con conexión a internet a través de un router ADSL
- Equipos utilizados por los empleados de una empresa para el trabajo habitual.
- Sistemas operativos:
  - Windows
  - Linux
  - iOS
  - Android

Ejercicio:
Estudiar las versiones que se utilizan actualmente de estos SO

Equipos **servidor** con conexión a Internet

- Equipo utilizado para ejecutar un programa (proceso servicio) que está pendiente de atender (dar servicio) a otros equipos que lo soliciten.
- Los servicios pueden ser utilizados dentro de la red de la empresa (LAN) o fuera de ella (desde Internet).
- Sistemas operativos:
  - Windows
  - Linux
  - Otros…
- Implementación:
  - Máquina real
  - Virtualización – Máquina virtual
  - Contenedores

Ejercicio:
Estudiar las versiones que se utilizan actualmente de estos SO

Hardware **cliente - servidor** Configuración y precio

- Equipo cliente utilizado en un puesto de trabajo de un empleado de la empresa.
- Equipo servidor utilizado para alojar alguno de los servicios ofrecidos en la red de la empresa.
- Equipo cliente – smartphone para los empleados
- Impresora de red para la empresa.
- SAI para el apoyo eléctrico de un servidor
- Disco duro, Disco SSD.
- Tarjetas gráficas especiales,…

Ejercicio:
Estudiar la configuración y el precio del equipo necesario para una de estas necesidades

Software **cliente** (Windows / Linux) Configuración segura

- Sistema Operativo actualizado
- Configuración inicial correcta: Nombre, conf de red, servidor DNS, …
- Separar cuenta de usuario normal (para el trabajo habitual) de la cuenta de usuario administrador (para la instalación y administración del equipo). Crear una cuenta administrativa de reserva.
- Antivirus – Antimalware (actualizado y activo)
- Cortafuegos local
  - Permitir la salida a Internet y la entrada de las consultas
  - No permitir la entrada a nuestro equipo desde Internet – Administración remota segura y controlada si es necesario
- Configuración segura del navegador (s) utilizado (En todas las cuentas de usuario)
- Separar partición de datos y de sistema.
- Creación de una imagen del sistema o punto de restauración
- Cifrado de información sensible almacenada en este equipo
- Gestión segura de certificados digitales
- Utilización de la firma digital
- Mantener monitorizado el equipo y limpio de ficheros temporales…

Software **cliente** (Windows / Linux)

Orden de trabajo en la máquina

ORDEN DE TRABAJO EN LA MÁQUINA xxxW750 - xxxWX50 - xxxLM51 xxxW7Limpia – xxxWXLimpia - xxxLMLimpia

1. **Clono** la máquina limpia WXLimpia o instalo el SO desde 0.
2. **Arranco** la máquina
3. Cambio el **nombre** a xxxWX50
4. **Configuro** la tarjeta de **red**
5. Compruebo la **conectividad** con Internet
6. Compruebo **actualizaciones** del SO, **particiones**, **memoria**… y **reinicio** la máquina
7. Creo una cuenta **miadmin2** de reserva (cuenta administradora)
8. Creo las **cuentas locales** que necesite: cuentas no administrativas para los usuarios del equipo (solo cuando el equipo no vaya a estar en Active Directory)
9. Compruebo que está deshabilitada la administración remota de esta máquina.
10. Habilito el servicio de firewall de Windows (si es necesario abro la entrada al protocolo ICMPv4)
11. Instalo - compruebo y actualizo el **Antivirus - Antimalware**
12. Instalo y configuro los programas que necesite el usuario: (Navegador, …)
13. Creo una carpeta compartida en la partición de datos (**CompartidaFuera**) a la que podrá conectarse todos los que conozcan la cuenta (**forastero**/forastero)

Software **cliente** (Windows / Linux)
Ejercicios prácticos posibles

- **Cambiar el destino de la carpeta de usuario a la partición de datos**
- **Probar distintos programas antimalware**
- **Probar programas de cifrado simétrico**
- **Probar la creación de certificados digitales**
  - Probar el cifrado asimétrico
  - Probar la firma digital
- **Probar distintas configuraciones de particiones, discos, RAID (se utiliza en un servidor)**
- **Conectar y configurar un SAI (se suele utilizar en un servidor)**
- **Monitorización del sistema – procesos que se están ejecutando en el equipo**
- **Habilitar y probar la administración remota**
  - Administración remota basada en un servidor externo https
- **Probar un software de copia de seguridad y restauración de la copia**
- **Realizar una imagen del sistema y recuperar una imagen**
- **Configuración segura de recursos compartidos**
  - Compartir recursos entre plataformas Linux y Windows - SAMBA

Software **cliente de empresa** Configuración segura

- Sistema Operativo actualizado
- Configuración inicial correcta: Nombre, conf de red, servidor DNS, …
- Crear una cuenta administrativa de reserva.
- Meter el equipo en el dominio de AD / LDAP para poder utilizar las cuentas de dominio
- Antivirus – Antimalware (actualizado y activo)
- Cortafuegos local
  - Permitir la salida a Internet y la entrada de las consultas
  - No permitir la entrada a nuestro equipo desde Internet – Administración remota segura y controlada si es necesario
- Configuración segura del navegador (s) utilizado (En todas las cuentas de usuario)
- Normalmente no almacenaremos información de la empresa en estos equipos, por tanto no será necesaria la partición de datos.
- Creación de una imagen del sistema o punto de restauración
- Gestión segura de certificados digitales
- Utilización de la firma digital
- Mantener monitorizado el equipo y limpio de ficheros temporales…

Software **servidor** (Windows / Linux) Configuración segura

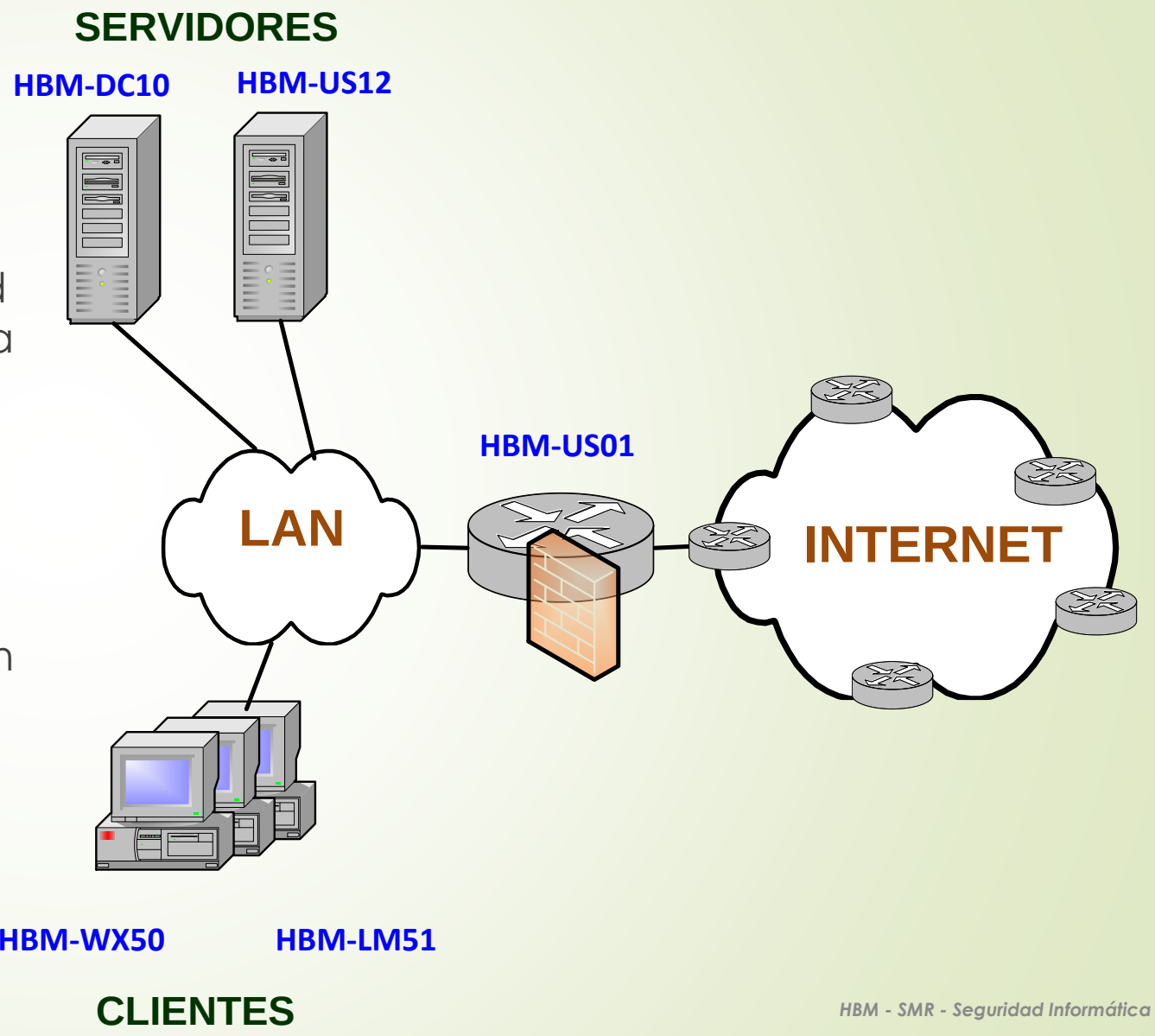
- Sistema Operativo actualizado
- Configuración inicial correcta: Nombre, conf de red, servidor DNS, …
- Crear una cuenta administrativa de reserva.
- Antivirus – Antimalware (actualizado y activo)
- Cortafuegos local
  - Permitir la salida a Internet y la entrada de las consultas
  - No permitir la entrada a nuestro equipo desde Internet – Administración remota segura y controlada si es necesario
- Configuración segura del navegador (s) utilizado (En todas las cuentas de usuario)
- Separar partición de datos y de sistema.
- Creación de una imagen del sistema o punto de restauración
- Cifrado de información sensible almacenada en este equipo
- Gestión segura de certificados digitales
- Utilización de la firma digital
- Mantener monitorizado el equipo y limpio de ficheros temporales…

Software **servicio** (Windows / Linux) Configuración segura

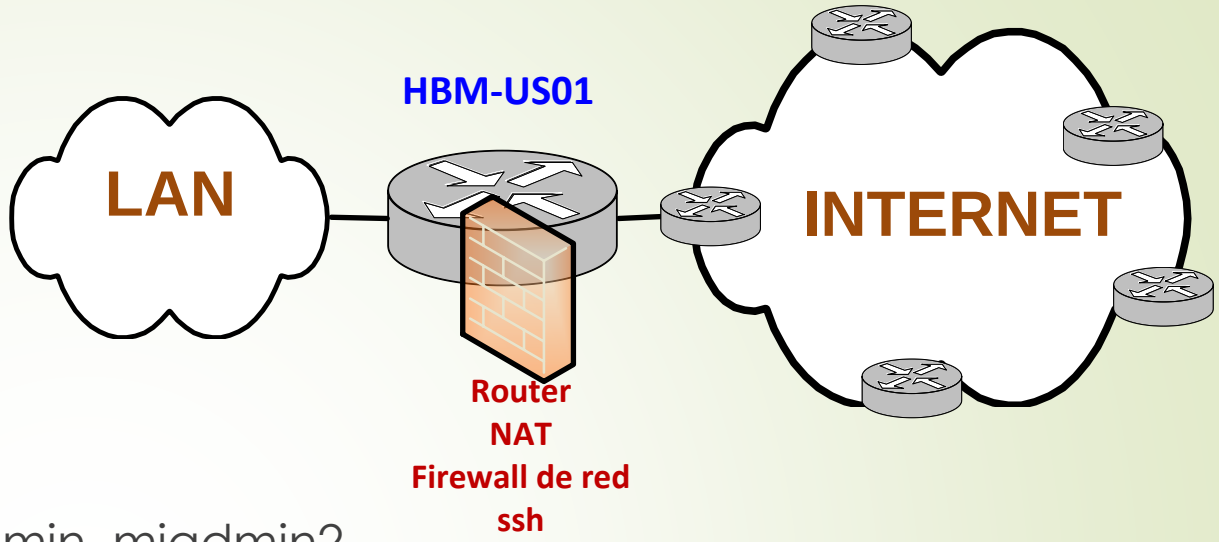
- Actualizar el sistema operativo y comprobaciones previas a la instalación
- Instalación del servicio
- Configuración del servicio, documentación y copia de seguridad de los ficheros de configuración
- (En el cliente: equipo que va a utilizar el servicio) Configuración del cliente
- Prueba del servicio (desde el cliente)
- Monitorización y actualización del servicio para su correcto funcionamiento y rendimiento

Mi empresa

- Un **router** – cortafuegos de red para la conexión y salida de la empresa a Internet
- Una red local - **LAN**
- Dos **servidores** internos, uno Windows y otro Linux
- Los **equipos cliente** que utilizan los empleados de la empresa
- Una **impresora de red**, **teléfonos IP**,…

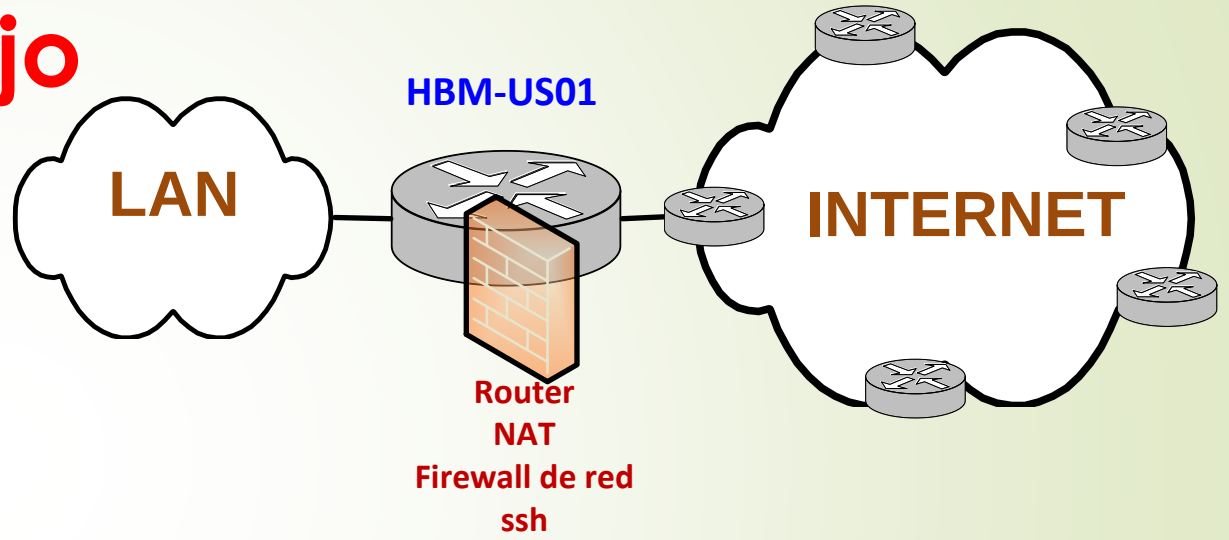


HBM-US01



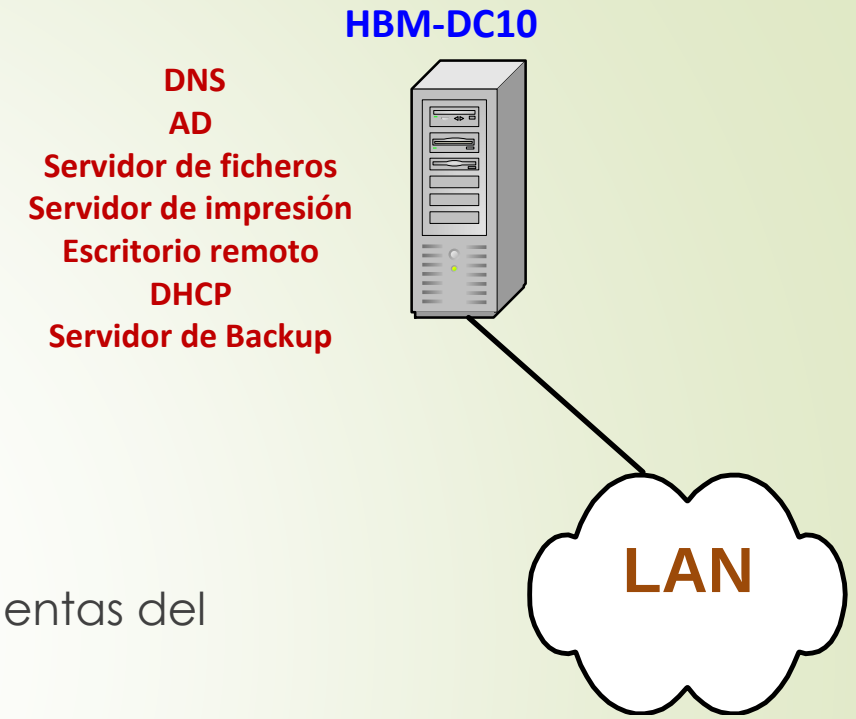
- Sistema operativo: Ubuntu Server
- Dos cuentas administradoras: miadmin, miadmin2
- Dos tarjetas de red: una conectada a la LAN y otra conectada a Internet
- Servicio de enrutamiento activado (**router**)
- **NAT** en la tarjeta de red conectada a Internet
- Administración remota (**ssh**) habilitada desde algún equipo de la LAN de la empresa
- **Cortafuegos de red** UFW configurador en esta máquina

HBM-US01
Orden de trabajo



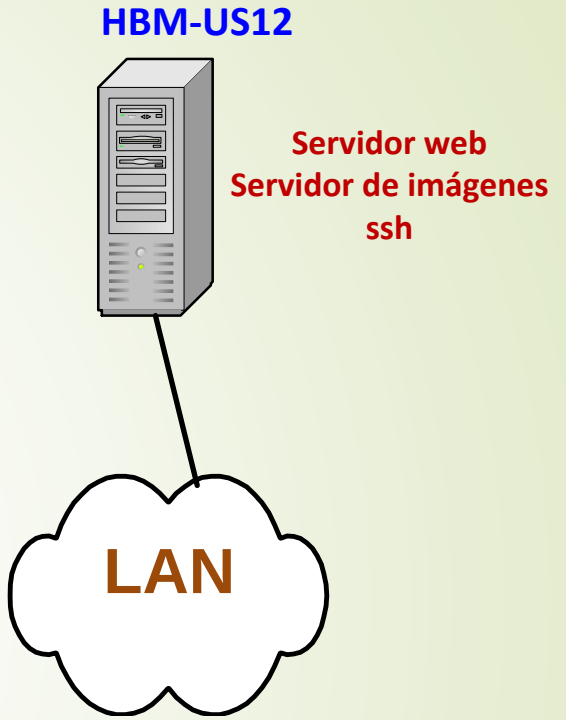
1. **Clono** la máquina limpia USLimpia
2. Pongo **dos tarjetas de red** a la máquina
3. **Arranco** la máquina
4. Cambio el **nombre** a xxxUS01
5. **Configuro** las dos tarjetas de **red**
6. Compruebo la **conectividad** con internet
7. Compruebo **actualizaciones** del SO, **particiones**, **memoria**… y **reinicio** la máquina
8. Creo una cuenta **miadmin2** de reserva (cuenta administradora de reserva)
9. Habilito y pruebo el **servicio SSH** (desde la máquina 50 o desde el anfitrión)
10. Habilito y pruebo el **servicio de enrutamiento**
11. Habilito el servicio de firewall (**UFW**)
12. Configuro ufw para que haga **NAT**
13. **Estudio y documento ufw**

HBM-DC10



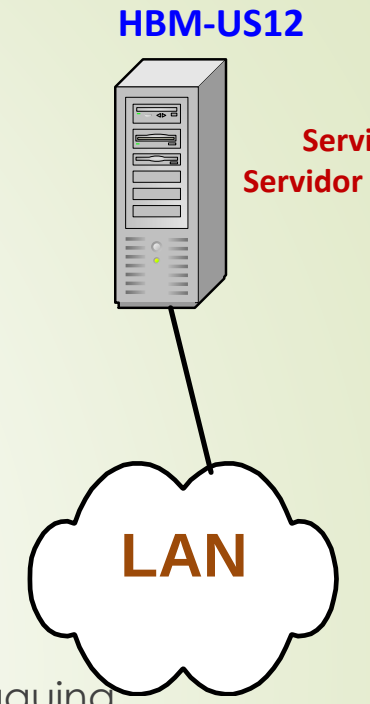
- Sistema operativo: Windows 19 Server
- Dos cuentas administradoras: Administrador, miadmin
- Una tarjeta de red conectada a la LAN
- Antivirus y cortafuegos local habilitados
- Habilitada la conexión por escritorio remoto para las cuentas del grupo operadores y las cuentas administradoras
- Servicio **DNS** en el dominio *midominio.local*
- Servicio **AD** para el dominio *midominio.local*
  - Creación de las cuentas de dominio necesarias para la empresa
- **Servidor de ficheros** para los clientes de la empresa
  - Configuración de los permisos de acceso a la estructura de ficheros
- **Servidor de Backup** para los datos de la empresa
- **Servidor de impresión** para los clientes de la empresa

HBM-US12



- Sistema operativo: Ubuntu Server
- Dos cuentas administradoras: miadmin, miadmin2
- Una tarjeta de red conectada a la LAN
- Antivirus y cortafuegos local habilitados
- Habilitada la administración remota por ssh para algún equipo de la LAN
- **Servidor de web** para los clientes de la empresa
  - Cuenta para administrar los contenidos web: *operadorweb*
- **Servidor de imágenes** para los datos de la empresa
  - Cuenta para administrar y utilizar las imágenes: *operadorimagen*

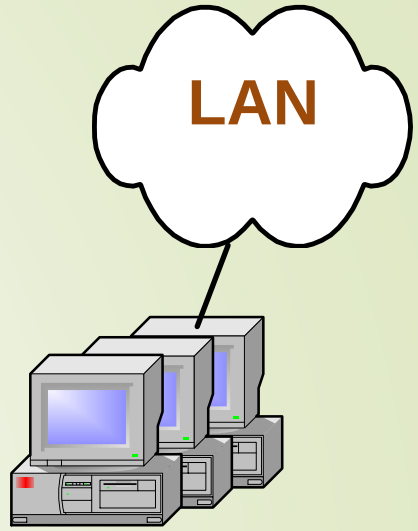
HBM-US12
Orden de trabajo



1. **Clono** la máquina limpia USLimpia
2. **Arranco** la máquina
3. Cambio el **nombre** a xxxUS12
4. **Configuro** la tarjeta de **red**
5. Compruebo la **conectividad** con internet
6. Compruebo **actualizaciones** del SO, **particiones**, **memoria**… y **reinicio** la máquina
7. Creo una cuenta **miadmin2** de reserva (cuenta administradora de reserva).
8. Habilito y pruebo el **servicio SSH** (desde la máquina 50 o desde el anfitrión)
9. Instalamos, configuramos y probamos el servicio HTTP
10. Crear la cuenta **operadorweb** y darle permisos en la carpeta /var/www/html/
11. **Probar** la cuenta operadorweb modificando el index.html desde la máquina 50 utilizando Filezilla con una conexión **sftp**.
12. Crear la cuenta **operadorimagen** y darle permisos en /var/imagenes/
13. Habilito el servicio de firewall (**ufw**)
14. **Estudio y documento ufw**

HBM-WX50

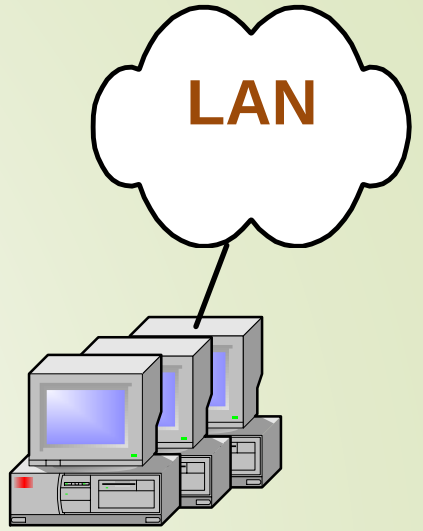
- Sistema operativo: Windows X
- Dos cuentas administradoras: Administrador, miadmin
- Una tarjeta de red conectada a la LAN
- Antivirus y cortafuegos local habilitados
- El equipo pertenece al dominio de AD de la empresa
- Cliente DNS
- Cliente AD donde podemos utilizar todas las cuentas de dominio
- Cliente del Servidor de ficheros
- Cliente del servidor de impresión
- Cliente del servidor Web
- Cliente del router y firewall de red



HBM-LM51

- Sistema operativo: Linux Mint
- Dos cuentas administradoras: miadmin, miadmin2
- Una tarjeta de red conectada a la LAN
- Antivirus y cortafuegos local habilitados
- El equipo pertenece al dominio de AD de la empresa
- Cliente DNS
- Cliente AD donde podemos utilizar todas las cuentas de dominio
- Cliente del Servidor de ficheros
- Cliente del servidor de impresión
- Cliente del servidor Web
- Cliente del router y firewall de red

Cliente DNS
Cliente AD
Cliente del servidor de ficheros
Cliente del servidor de impresión
Cliente DHCP
Cliente escritorio remoto
Cliente ssh
Cliente web



HBM-LM51

Otras alternativas de implantación

- Utilizar otros sistemas operativos
- Utilizar solo servidores Linux… utilizaríamos LDAP en lugar de AD
- Utilización de SAMBA para servidor de ficheros Linux con clientes Windows
- Servidor de impresión en Linux
- Utilización de un proxy web para filtrar y vigilar el trafico web de los empleados
- Utilizar almacenamiento den la nube para las copias de seguridad.
- Utilizar almacenamiento en la nube para colocar nuestros servidores – servicios
  - Virtualización
  - Contenedores

Estructura del libro de seguridad

- /aammddLibroDeEjerciciosHeraclio/
  - Leeme.txt
  - ComandosYFicherosUtilizados.odt
  - EjerciciosTema1SeguridadInformática.odt
  - EjerciciosTema2HardwareDeSeguridad.odt
  - EjerciciosTema3CopiaDeSeguridad.odt
  - EjerciciosTema4Criptografía.odt
  - EjerciciosTema5MonitorizaciónSistema.odt
  - EjerciciosTema6MonitorizaciónRed.odt
  - EjerciciosTema7UFW.odt
  - EjerciciosTema8SQUID.odt
  - EjerciciosTema9Legislación.odt
  - …
- /ExamenPráctico1-Hogar/
  - HBM-WX50.odt
  - HBM-LM51.odt
- /ExamenPráctico2-3-Empresa/
  - Empresa.odt
  - HBM-US01.odt
  - HBM-US12.odt
  - HBM-DC10.odt
  - HBM-DC20.odt
  - HBM-WX50.odt
  - HBM-LM51.odt
  - /DocumentacionExtra/
  - …

Seguimiento del examen práctico

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
PRESUPUESTO						
SISTEMA OPERATIVO						
NOMBRE						
CONF. DE RED						
CUENTAS LOCALES						
DISCO - PARTICIONES						
ANTIMALWARE						
FIREWALL LOCAL						Abrir ICMP. Firewall de Windows. UFW en Linux
ADM. REMOTA SEGURA	C	C	S	S	S	Escritorio remoto en Windows. SSH en Linux
IMAGEN DEL SISTEMA	C	C		S		Utilizando Clonezilla
COPIA DE SEGURIDAD			S			Utilizando Cobian Backup
DHCP	C	C	S			
DNS	C	C	S	C	C	
AD			S			
- Clientes AD	C	C	S			
- Cuentas AD	C	C	S			
SERVIDOR DE FICHEROS	C	C	S			
SERV. DE IMPRESIÓN	C	C	S			
SERVIDOR WEB	C	C	C	S		
ROUTER	C	C	C	C	S	
NAT	C	C	C	C	S	
FIREWALL DE RED	C	C	C	C	S	UFW en el router
MONITOR DE SISTEMA						
MONITOR DE RED						
DOCUMENTACIÓN						
DOC. DE LA EMPRESA						

Seguimiento del examen práctico

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
PRESUPUESTO						
SISTEMA OPERATIVO						
NOMBRE						
CONF. DE RED						
CUENTAS LOCALES						
DISCO - PARTICIONES						
ANTIMALWARE						
FIREWALL LOCAL						Abrir ICMP. Firewall de Windows. UFW en Linux
ADM. REMOTA SEGURA	C	C	S	S	S	Escritorio remoto en Windows. SSH en Linux
IMAGEN DEL SISTEMA	C	C		S		Utilizando Clonezilla
COPIA DE SEGURIDAD			S			Utilizando Cobian Backup
DHCP	C	C	S			
DNS	C	C	S	C	C	
AD			S			
- Clientes AD	C	C	S			
- Cuentas AD	C	C	S			
SERVIDOR DE FICHEROS	C	C	S			
SERV. DE IMPRESIÓN	C	C	S			
SERVIDOR WEB	C	C	C	S		
ROUTER	C	C	C	C	S	
NAT	C	C	C	C	S	
FIREWALL DE RED	C	C	C	C	S	UFW en el router
MONITOR DE SISTEMA						
MONITOR DE RED						
DOCUMENTACIÓN						
DOC. DE LA EMPRESA						

Configuración inicial de las máquinas

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
PRESUPUESTO						
SISTEMA OPERATIVO						
NOMBRE						
CONF. DE RED						
CUENTAS LOCALES						
DISCO - PARTICIONES						
ANTIMALWARE						
FIREWALL LOCAL						Abrir ICMP. Firewall de Windows. UFW en Linux

Enrutamiento y NAT
Firewall de red

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
ROUTER	C	C	C	C	S	
NAT	C	C	C	C	S	
FIREWALL DE RED	C	C	C	C	S	UFW en el router

- Configuración del servicio de enrutamiento
- Configuración de NAT en la tarjeta exterior del router
- Comprobación del servicio de enrutamiento
- Comprobación de NAT
- Prueba desde los clientes

Administración remota segura

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
ADM. REMOTA SEGURA	C	C	S	S	S	Escritorio remoto en Windows. SSH en Linux

- Instalación del servicio **SSH** en los equipos Linux
- Habilitar **escritorio remoto** en los equipos Windows
- Configurar los firewall de los servidores para que permitan el acceso autorizado
- Prueba desde los clientes con el software adecuado:
  - **Putty** para conectar a equipos Linux
  - **Conexión a escritorio remoto** para conectar a equipos Windows

DNS

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
DNS	C	C	S	C	C	

- Instalación del servicio ***midominio.local***
- Configuración adecuada de la zona directa e inversa
- Copia de seguridad de los ficheros de configuración
- Monitorización del servicio
- Configuración de los clientes para que utilicen el servidor. Configuración del sufijo DNS y del dominio de búsqueda en los clientes.
- Prueba desde los clientes.

AD – ACTIVE DIRECTORY

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
AD			S			
- Clientes AD	C	C	S			
- Cuentas AD	C	C	S			

- Instalación del servicio de AD
- Meter los clientes en el dominio de AD
- Crear y configurar las cuentas y grupos del dominio de AD
  - (**jefe1**, **jefe2**, **currito1**, **currito2**, **operadorcopia**, **operadordominio**,…)
- Configurar las directivas de dominio adecuadas (una vez creada la estructura de ficheros, recursos compartidos y permisos adecuados)
- Probar las cuentas desde el cliente Windosws
- Probar las cuentas desde el cliente Linux

SERVIDOR DE FICHEROS

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
SERVIDOR DE FICHEROS	C	C	S			

- Instalación del servicio – configuración de los recursos compartidos
- Configuración de los permisos siguiendo las especificaciones. Control de acceso a los recursos.
- Utilización de los recursos compartidos desde un equipo Windows
- Utilización de los recursos compartidos desde un equipo Linux

COPIA DE SEGURIDAD COBIAN BACKUP

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
COPIA DE SEGURIDAD			S			Utilizando Cobian Backup

- Creación de la cuenta **operadorcopia** para gestionar este servicio
- Instalación del servicio Cobian Backup
- Configuración de las tareas de copia – política de copa de seguridad.
- Monitorización de la realización de las copias
- Recuperación de una copia o de una parte de una copia

IMAGEN DEL SISTEMA CLONEZILLA

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
IMAGEN DEL SISTEMA	C	C		S		Utilizando Clonezilla

- Creación de la cuenta **operadorimagen** para gestionar este servicio
- Utilizando Clonezilla realizar la imagen de la máquina 50 / 51 sobre el servidor de imágenes (máquina 12)
- Utilizando Clonezilla realizar la recuperación imagen de la máquina 50 / 51 desde el servidor de imágenes (máquina 12) sobre una máquina limpia

DHCP

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
DHCP	C	C	S			

- Instalación del servicio
- Configurar un ámbito y una reserva de MAC para las máquinas 50 y 51 con los identificadores de host 60 y 61
- Copia de seguridad de los ficheros de configuración
- Monitorización del servicio
- Probar el servicio desde los clientes 50 y 51

SERVIDOR WEB

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
SERVIDOR WEB	C	C	C	S		

- Instalación del servicio
- Configuración
- Copia de seguridad de los ficheros de configuración
- Monitorización del servicio

SERVIDOR DE IMPRESIÓN

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
SERV. DE IMPRESIÓN	C	C	S			

- Instalación del servicio
- Configuración
- Copia de seguridad de los ficheros de configuración
- Monitorización del servicio

MONITORIZACIÓN Y DOCUMENTACIÓN

FECHA:	MÁQUINAS					OBSERVACIONES
TRABAJO	50	51	10	12	01	
MONITOR DE SISTEMA						
MONITOR DE RED						
DOCUMENTACIÓN						
DOC. DE LA EMPRESA						

- Monitorización de cada máquina para comprobar que funciona correctamente, la máquina y los servicios que corren sobre ella
- Monitorización de la red de la empresa para vigilar el tráfico y la carga de trabajo
- Documentación de todas las actuaciones sobre cada maquina
- Documentación general de la empresa
  - Plano de red

De todo quedaron tres cosas:

la certeza de que estaba siempre comenzando,
la certeza de que había que seguir
y la certeza de que sería interrumpido antes de terminar.
Hacer de la interrupción un camino nuevo,
hacer de la caída, un paso de danza,
del miedo, una escalera,
del sueño, un puente,
de la búsqueda,…un encuentro.

- Fernando Pessoa