Documento pendiente de unificar el contenido

TRABAJO INICIAL PARA LA PREPARACIÓN DE LA EMPRESA

DOCUMENTACIÓN DEL MODELO DE RED – PLANO DE RED DE LA EMPRESA

INSTALACIÓN DEL SISTEMA OPERATIVO

PARTICIONES:

Sistema y Datos	(Para los clientes windows)
/ y /home	(Para los clientes Linux Mint)
Sistema, Datos y Backup	(Para Windows 2012 server)
/ y /var	(Para Ubuntu Server)

NOMBRE Y CONFIGURACIÓN DE RED DE LAS MÁQUINAS

CONTROL DE ACCESOS – CUENTAS LOCALES:

Administrador y admin	(Para los clientes windows)
miadmin y miadmin2	(Para los clientes Linux Mint)
Administrador y admin	(Para Windows 2012 server)
miadmin y miadmin2	(Para Ubuntu Server)

ANTIVIRUS:

Essentials	(Para los clientes windows)
clamtk	(Para los clientes Linux Mint)
Essentials	(Para Windows 2012 server)
ClamAV	(Para Ubuntu Server)

CORTAFUEGOS LOCAL:

Firewall de Windows	(Para los clientes windows)
ufw	(Para los clientes Linux Mint)
Firewall de Windows	(Para Windows 2012 server)
IPTABLES	(Para Ubuntu Server)

Politica:

- Trafico saliente: permitir
- Trafico entrante: denegar
  - Excepción: permitir entrante ICMP

MONITOR DEL SISTEMA:

ESCANER DE PUERTOS:

SIMULACIÓN DE ATAQUE:

COPIA DE SEGURIDAD DE FICHEROS DE CONFIGURACIÓN:

/etc/isue
/etc/fstab
/etc/hosts
/etc/hostname
/etc/passwd
/etc/group
/etc/network/interfaces
/etc/sys/net/ipv4/ip_forward
/etc/sysctl.conf
/etc/rc.local
/etc/samba/smb.conf

CONFIGURACIÓN DE LAS MÁQUINAS LIMPIAS UTILIZADAS EN LOS EJERCICIOS DE SEGURIDAD

Todas con una tarjeta de red en adaptador puente y las guest additions instaladas.

S.O.	Arquitectura	Memoria RAM	Disco Duro (HD)	Particiones	Cuentas locales	Aplicaciones	Configuración adicional
Windows 7 Profesional	32 Bits	1 GB	500 GB	Sistema → 150 GB Datos → 350 GB	admin/Aaa111!!! administrador/Aaa111!!!	Antivirus Firefox Notepad ++ Putty Filezilla	Sin actualizaciones automáticas Cortafuegos activado(ICMP abierto)
Linux mint 17.2	32 Bits	1 GB	500 GB	Sistema / → 150 GB Datos (/home/) → 350GB Swap 8 GB	admin/Aaa111!!! admin2/Aaa111!!!	Antivirus	Actualizar repositorios: update y upgrade
Ubuntu Server 14.04	64 Bits	1 GB	500 GB	Sistema (/) → 150 Gb Swap 8 Gb Datos (/var/) → 350 GB	admin/Aaa111!!! admin2/Aaa111!!!	SSH Server	Actualizar repositorios: update y upgrade
Windows Server 2012 R2	64 Bits	2 GB	500 GB	Arranque → 350 GB Sistema → 200 GB Datos → 150 GB Backup → 150 GB	administrador/Aaa111!!! admin/Aaa111!!!	Firefox Notepad ++ Putty Filezilla	Sin actualizaciones automáticas Cortafuegos activado(ICMP abierto)

SEGUIMIENTO Y PRUEBA DEL EXAMEN PRÁCTICO DE SEGURIDAD

Documentación general para un servicio:

SERVIDOR:

- **Instalación** del servicio
- **Configuración** del servicio
- **Mantenimiento** (arrancar, parar, reiniciar,ver el estado, …)
- **Log** del servicio
- **Copia de seguridad** (Configuración, log,…)
- **Alta disponibilidad**, replicar

CLIENTE

- **Prueba** del servicio

Documentación para una máquina:

(Programas, servicios y clientes disponibles en la máquina)

- **Sistema operativo**
- **Nombre**
- **Configuración de red** (estática, dinámica, alternativa, automática)
- **Cuentas locales** (cuentas, certificados, tarjetas, ...)
- **Particiones**
- **Programas** instalados: Antivirus, navegador, editor, …
- **DNS**
- **Comunicaciones**: Router, NAT, Cortafuegos (local y de red), Proxy, ...
- **AD**
  - Equipos
  - OU, Grupos, Cuentas
  - GPO
- **Administración remota segura**
- **Servidor de ficheros**, DFS
- **Recursos Compartidos**
- **Servidor de impresión**
- Servidor de backup e imágenes: **Copia de seguridad**
- **Servidor web**: HTTP, HTTPS, SFTP,…
- **VPN** de acceso remoto, VPN punto a punto
- **VLAN**
- WI-FI segura, **portal cautivo**

	G_Jefes	G_Curritos	Todos
GPO_Defaul domain policy			V:\BandejaDeImpresion\ W:\DocumentosRecuperados
GPO_InicioJefes	X:\ComunCurritos\ Y:\ComunJefes		
GPO_InicioCurritos		X:\ComunCurritos\	
ConfDeCuenta			Z:\CarpetaPersonal

Pendiente incluir aquí la propuesta de AD y de servidor de ficheros para la empresa.