delivering value

Hardening: alta seguridad bajo Win32

Andrés Tarascó Acuña
atarasco@sia.es

sia

delivering value

INDICE

- **Introducción. ¿Qué es el Hardening?**
  - Mitigar los vectores de ataque
- **Prevención de ataques – Medidas básicas**
  - Fortificación de cuentas de usuario
  - Fortificación del sistema operativo
  - Dispositivos (prevención de acceso físico)
- **Prevención de ataques - Medidas avanzadas**
  - Uso de Firewalls en la DMZ
  - Protecciones ante ejecución de código
  - Accesos remotos
  - Cifrado de disco
  - Buenas prácticas

¿Qué es el Hardening?

Configuración robusta del sistema operativo.

¿Qué queremos conseguir?

- Proteger el sistema contra ataques y accesos no autorizados
- Prevenir el mal uso del sistema de los usuarios,
- Prevenir la pérdida de información y caídas del sistema.
- Evitar vectores de ataques conocidos
- Limitar el impacto de vulnerabilidades 0day
- No perder totalmente la funcionalidad del sistema
- Mejorar el rendimiento global

Introducción – Hardening

¿Qué podemos conseguir realmente?

Inmunizar el sistema contra ataques conocidos

Maximizar el tiempo necesario para llevar a cabo un ataque en la plataforma

Evitar el robo de información en el sistema

Hardening básico – Cuentas de usuario

- **Fortificación de cuentas de usuario**
  - Definición de roles restringidos
  - Política de contraseñas eficiente
  - Políticas de acceso restrictivas en base a grupos (secpol)

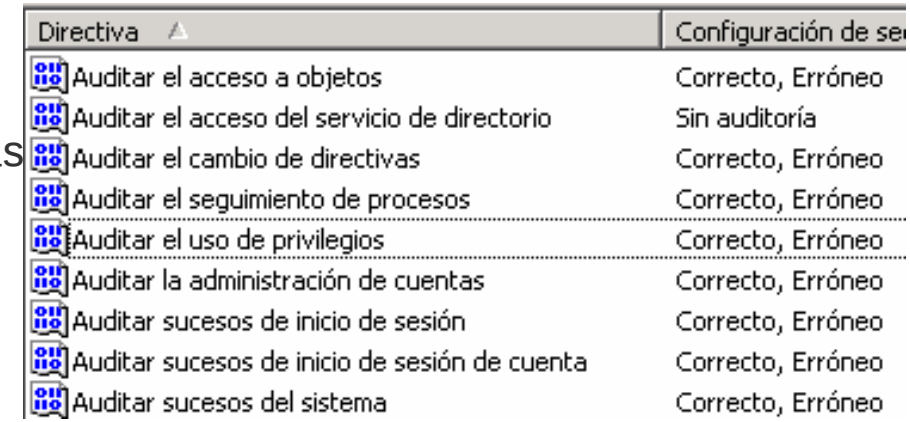
Directiva	Configuración de seguridad
Almacenar contraseña usando cifrado reversible...	Deshabilitada
Forzar el historial de contraseñas	24 contraseñas recordadas
Las contraseñas deben cumplir los requerimiento...	Habilitada
Longitud mínima de la contraseña	8 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	2 días

Nombre	Descripción
Administradores	Los administradores tienen acceso c...
Duplicadores	Pueden duplicar archivos en un dominio
Invitados	Los Invitados tienen predeterminada...
Operadores de configuración de red	Los miembros en este equipo puede...
Operadores de copia	Los operadores de copia pueden sob...
Usuarios	Los usuarios no pueden hacer cambi...
Usuarios avanzados	Los usuarios avanzados tienen más ...
Usuarios de escritorio remoto	A los miembros de este grupo se les ...
Hardening-AccesoApplicaciones	Permisos de ejecución de Software
Hardening-ServiceAccounts	Cuentas de servicios del sistema
Hardening-Usuarios	Grupos de usuarios del sistema
HelpServicesGroup	Grupo para el Centro de ayuda y so...
Usuarios del depurador	Los usuarios del depurador pueden ...
__vmware__	VMware User Group

Cuentas no privilegiadas para servicios

Hardening básico – fortificación del sistema operativo

- **Fortificación del sistema operativo**
  - Gestión periódica de parches
    - Instalación: WSUS,SMS,BMC, CA PatchManagment, Patchlink..
    - Verificación: Mbsa, CA Assesment Management,BMC,..
  - Política de auditoría eficaz
    - Auditar inicios de sesión
    - Auditar cambios de políticas
    - Auditar Accesos a objetos



Directiva	Configuración de se
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso del servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Correcto, Erróneo
Auditar el seguimiento de procesos	Correcto, Erróneo
Auditar el uso de privilegios	Correcto, Erróneo
Auditar la administración de cuentas	Correcto, Erróneo
Auditar sucesos de inicio de sesión	Correcto, Erróneo
Auditar sucesos de inicio de sesión de cuenta	Correcto, Erróneo
Auditar sucesos del sistema	Correcto, Erróneo

  - Sincronización (W32time)
    - Correlación de eventos
    - Uso de servidores ntp confiables

```
D:\>net time /querysntp
El valor SNTP actual es: hora.rediris.es

Se ha completado el comando correctamente.
```

delivering value

Hardening básico – fortificación del sistema operativo

- **Fortificación del sistema operativo**
  - Auditar el acceso a cuentas falsas de usuario
    - Administrador / Administrator
  - Desinstalación de componentes no necesarios
    - Software del sistema operativo
    - Productos de terceros
    - Servicios innecesarios
  - Deshabilitar servicios del sistema no necesarios
    - Evaluar la funcionalidad del sistema.
  - Limitación de acceso al sistema de ficheros
    - Lectura: robo de credenciales
    - Escritura/Ejecución: Uso de exploits y backdoors.
  - Comunicationes seguras
    - NTLM2/SSL
    - IP estática
  - Hosts restringido

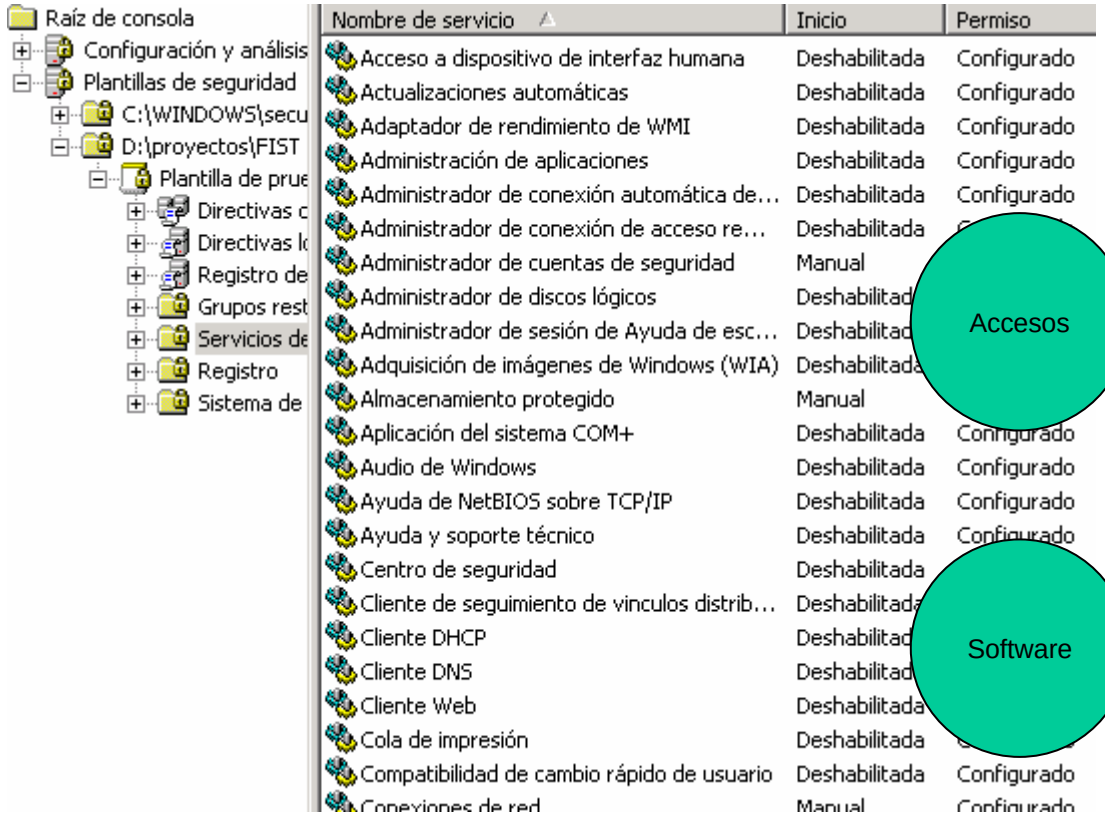
```
    0 System Process
    4 System
  656 smss.exe
  868 csrss.exe
  916 winlogon.exe
  964 services.exe
  976 lsass.exe
 1148 svchost.exe
 1304 svchost.exe
 1372 svchost.exe
 1528 svchost.exe
 1548 svchost.exe
 1796 spoolsv.exe
  788 explorer.exe
  368 cmd.exe
 2500 svchost.exe
```

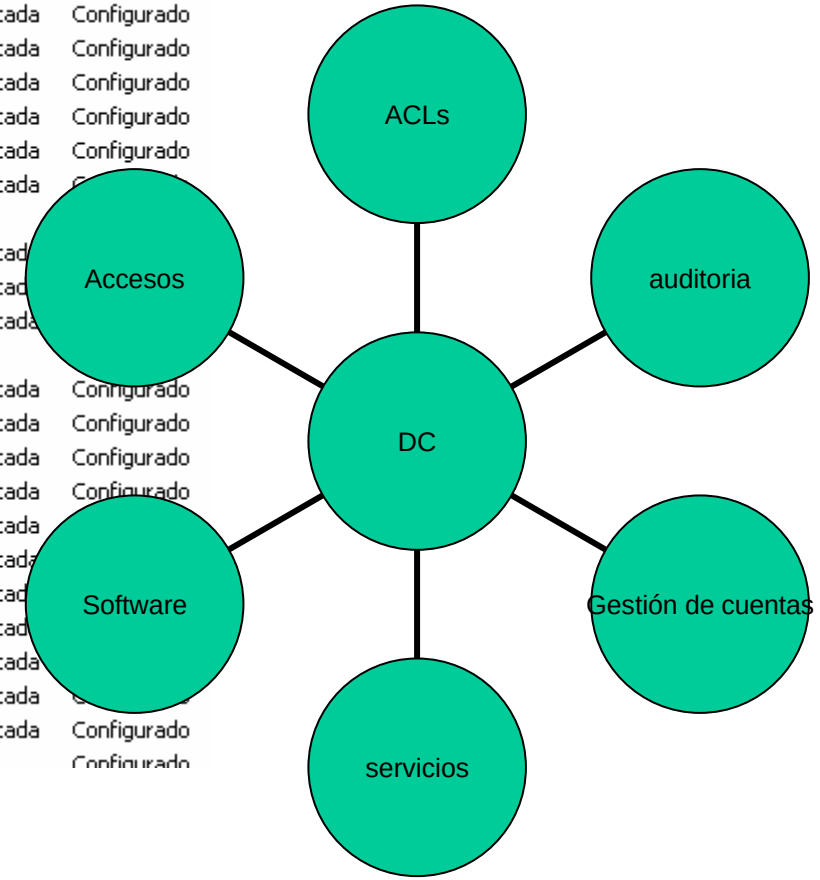
Hardening básico – prevención de ataques

- **Dispositivos y prevención de acceso**
  - Protector de pantalla
  - Limitar uso de dispositivos usb
  - Limitar acceso remoto a cdrom/floppy
  - Deshabilitar dispositivos de Hardware
    - Pantalla
    - Teclado
  - Ejecución automática.
    - autorun
  - Instalación de drivers no firmados

Hardening básico – Centralización de la seguridad

Gestión centralizada desde el controlador de dominio





Implantación de medidas técnicas

Hardening Avanzado

- Prevención de ataques - Medidas avanzadas
  - **Uso de Firewalls en la DMZ**
    - Integrado en interfaces de red
    - Ipsec (reglas de entrada y salida de tráfico)
    - Windows Firewall (definición de aplicaciones)
  - **Protecciones ante ejecución de código**
    - Windows DEP
    - Limitación dllcache/parches/Resource-Pack
    - Reglas de ejecución de software
  - **Accesos remotos**
    - Túneles SSH
    - Administrative shares
  - **Cifrado de disco**
    - Evitar acceso físico
    - Evitar integración en dominios
  - **Buenas prácticas**

Uso de firewalls en la infraestructura

- **Firewalls perimetrales**
  - Limitar ataques remotos
  - Limitar tráfico saliente
  - Monitorización de ataques (IDS / IPS)

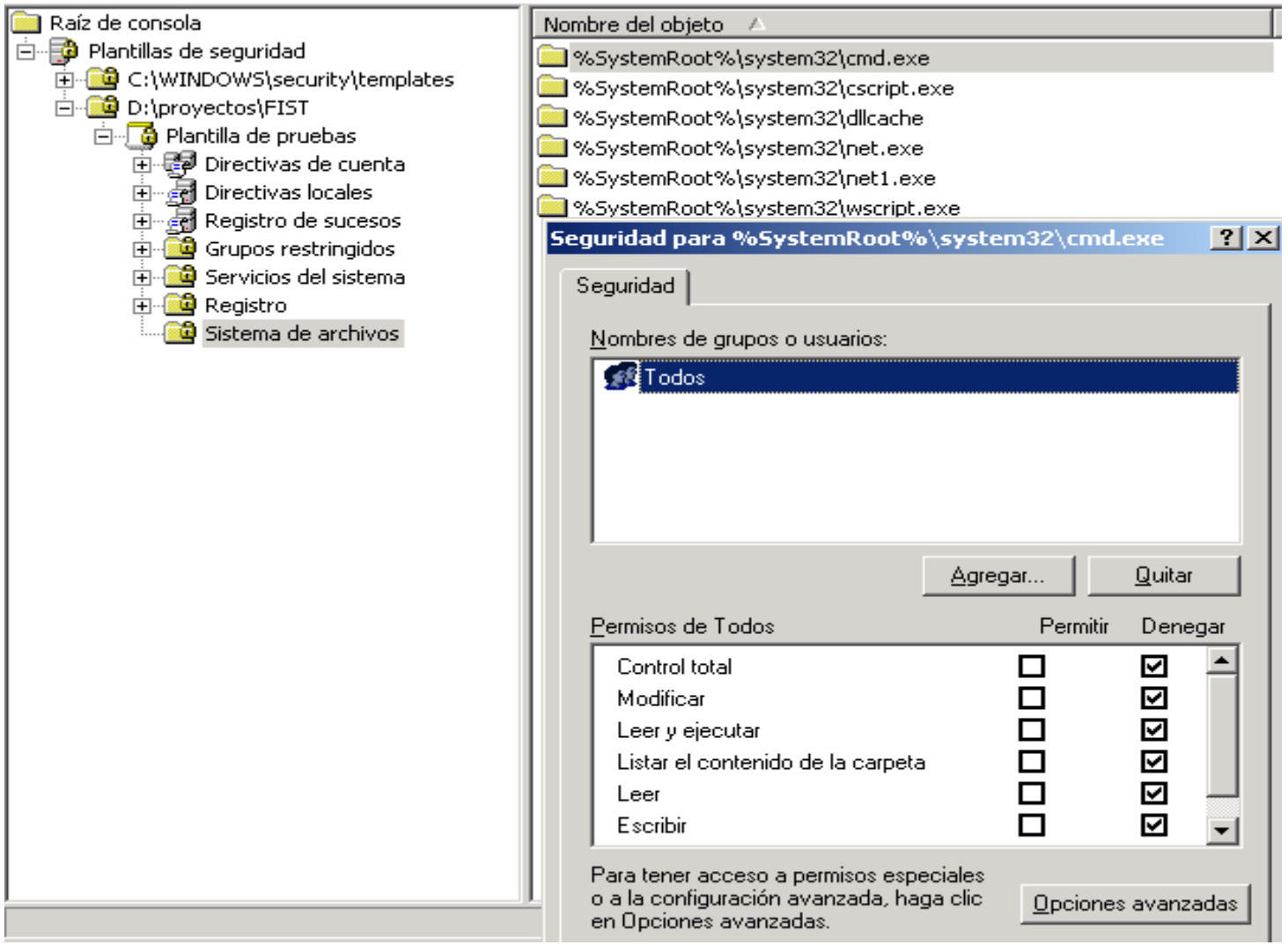
- **Firewalls locales (protección en la DMZ)**
  - Integrado en interfaces de red
    - Solo puertos autorizados
    - Evitamos backdoors en puertos aleatorios
  - Ipsec
    - reglas de entrada y salida de tráfico
    - Cifrado de comunicaciones
    - Evitamos conexiones a sistemas no autorizados
  - Windows Firewall
    - definición de aplicaciones válidas
    - Evitamos Shells en aplicaciones no definidas.

Hardening avanzado – Ejecución de código

- **Ejecución de código – ataques básicos.**
  - **Shell interactiva**
    - Limitar acceso a binarios (cmd,command,..)
  - **Transferencia de ficheros**
    - Limitar acceso a binarios - ftp,tftp,telnet,wscript
    - Limitar el acceso de escritura en disco
  - **Creación de usuarios**
    - Limitar acceso: net.exe, net1.exe
    - Políticas de acceso en base a usuarios (No grupos)
  - **Ejecución scripts .vbs, .wsh,..**
    - Limitar acceso a motores de scripting
  - **Varios: cacls, arp, ,ping, traceroute, route**
    - Limitar acceso para evitar information leak
  - **Inyección de código / VNC server**
    - Bloqueo automático de sesiones.
    - No guardar credenciales.

delivering value

Hardening avanzado – ejecución de código



Complemento *Plantillas de Seguridad*

Hardening avanzado – Ejecución de código

- **Impacto de las medidas en el sistema:**
  - **Acceso a aplicaciones necesario (.bat, .vbs,..)**
    - Scripts de inicio de sesión
    - Scripts en Webservers/Administración
  - **Perdida de funcionalidad. Soluciones:**
    - Crear copia de la aplicación con acceso restringido
      - Ejemplo: cmd.exe -> shell.exe
    - Definición de nuevas extensiones
      - Ejemplo: .bat -> .script
    - Asociación de nuevos binarios con nuevas extensiones
  - **Instalación de parches de seguridad fallidas**
    - Creación de scripts de marcha atrás
    - Habilitar auditoria -> acceso a objetos

Hardening avanzado – Ejecución de código

- **Formas genéricas de limitar ataques:**
  - **Eliminar contenido**: dllcache, parches ($NtUninstallKB*) , Resource-Packs
    - Son copias de seguridad peligrosas
    - Pueden ser utilizados para evitar protecciones de acceso
    - Revisión periódica (con cada parche instalado)
  - **Reglas de ejecución de software**
    - Solo permitir lo necesario.
    - No permitir ejecución donde haya permisos de escritura.
  - **Permisos heredables.**
    - Tener cuidado con permisos de Creator-owner (LocalService)
    - BypassTraverseChecking es nuestro amigo :)

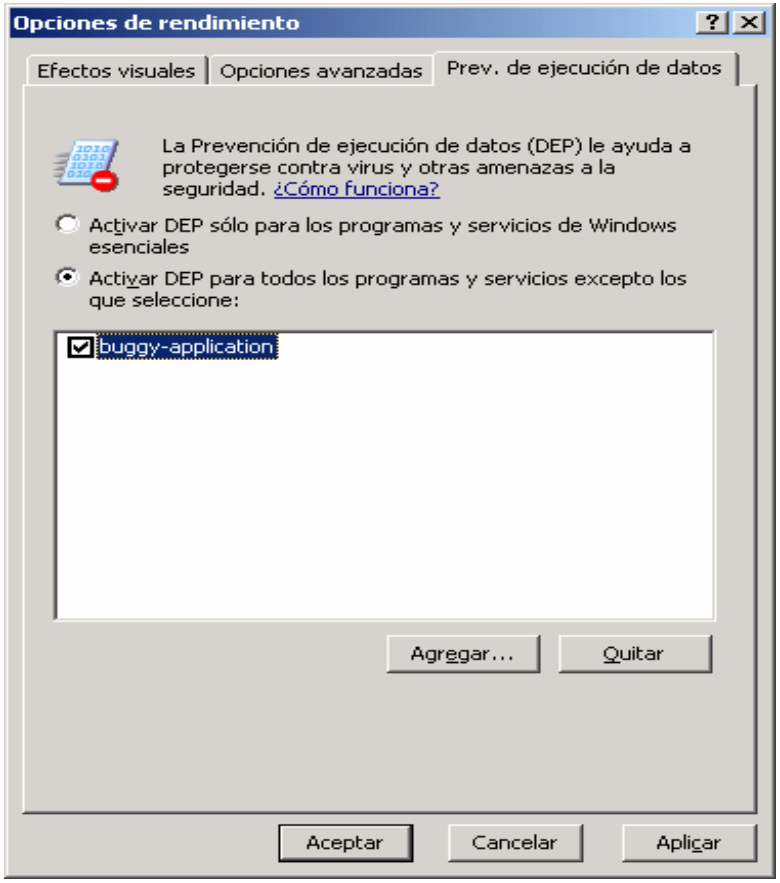
Hardening avanzado – Ejecución de código

- **Formas genéricas de limitar ataques:**
  - **Tecnología Windows DEP**

    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers

– Verificar:
  - Excepciones activas
  - MUICache *

(*)HKCU\Software\Microsoft\Windows\ShellNoRoam



- **Cifrado de disco**
  - **Evitar acceso en entornos multiusuario**
    - Cifrado de Windows integrado
    - Definición de un agente de recuperación
    - No integrar el sistema en el dominio
  - **Evitar acceso en dispositivos portátiles**
    - Habilitar password en el arranque del disco duro
  - **Evitar acceso offline**
    - Volumes cifrados (drivecrypt, bestcrypt,..)

Hardening Avanzado – Accesos remotos

- **Accesos remotos**
  - **Túneles SSH**
    - Filtrar todo el tráfico de entrada
    - Instalar servidor SSHD
      - Acceso mediante certificado y contraseña.
      - Servicio como LocalService / usuario
    - Redirección de puertos de acceso
      - Terminal server.
  - **Administrative shares**
    - Problemática con servicios de backup remoto
    - Definición de nuevos shares
      - XC$, XD$, Xadmin$
    - Limitación efectiva de ataques locales y remotos
      - Pwdump, dameware,...
  - Nuevas tecnologías
    - Microsoft NAP (Network access protection)
    - Cisco NAC (Network admission control)

Hardening Avanzado – Buenas prácticas

- **Buenas prácticas:**
  - **Evitar perfiles avanzados**
    - Trabajar como usuario
    - Usar cuentas administradores
  - **Desconfiar de la gestión de credenciales**
    - No usar Runas
    - Robo de credenciales en sesiones bloqueadas y desbloqueadas
    - Inyección de código en aplicaciones que usan otras credenciales (adm -> dom. Adm)
  - **Fortificación de contraseñas:**
    - Uso de caracteres Unicode
    - ÑÑÑÑÑÑÑÑÑ
  - **Borrado periódico del historial de comandos**

delivering value

RUEGOS Y PREGUNTAS
tic tac tic tac…

delivering value

Muchas Gracias