

Seguridad y Auditoría Informática

Auditoría de Sistemas Windows

Línea de Base de un Sistema

- Definir lo que constituye un sistema "seguro"
 - ... Y ver si el sistema analizado cumple con el estándar!
- Una vez que se tiene el sistema configurado, se toma una "línea de base" de esta configuración
- Periódicamente se restablece la línea de base y se buscan cambios.
- Esto permite monitorear problemas de seguridad a lo largo del tiempo.

Auditando en un Dominio Windows (1/3)

- Muchas organizaciones tienen un entorno de dominio de algún tamaño
- ¿Cómo impacta esto nuestra auditoría?
- Las buenas noticias:
 - Muchas herramientas funcionan igualmente bien en un sistema "single standalone" o un dominio de 10.000 equipos.
- Sin embargo, hay diferencias entre "standalone" y entornos de dominio...
 - Intentar consolidar y revisar los logs del *Event Viewer* de 10.000 equipos individuales Windows es una tarea desalentadora.
 - Intentar auditar apropiadamente permisos de archivos en un entorno grande con muchos grupos anidados puede ser desafiante.

Auditando en un Dominio Windows (2/3)

- En un equipo "standalone"
 - Toda la información está en el propio equipo
 - Es más simple para obtener la información sobre el sistema individual
 - Es más difícil obtener información sobre un gran número de sistemas individuales
 - Pero es aún posible.

Auditando en un Dominio Windows (3/3)

- En un entorno de dominio
 - La seguridad de un equipo está integrada con la seguridad del dominio.
- Lo que es más fácil:
 - Mucha información está ahora centralizada a nivel de dominio.
 - Usuarios, grupos, política de contraseñas, ...
- Lo que es más difícil:
 - La seguridad del cliente impactada por las configuraciones de dominio, por ejemplo Políticas de Grupo (*Group Policies*).
 - Seguridad aplicada en "capas" pueden complicar la auditoría (y la solución de problemas).
 - Problemas de Confianza de Dominio en grandes entornos multi-dominio.
 - Seguridad del sistema local debe aún ser abordada (por ejemplo, cuentas de dominio estándar como administradores locales)

Problemas No Técnicos

- Separación de Tareas
- Principio de Mínimo Privilegio
- Cuestiones de Procedimiento
 - Configuración de nuevas cuentas
 - Cambios de Contraseña
 - Política de Copias de Seguridad
 - Gestión de las Configuraciones

Esquema de Auditoría

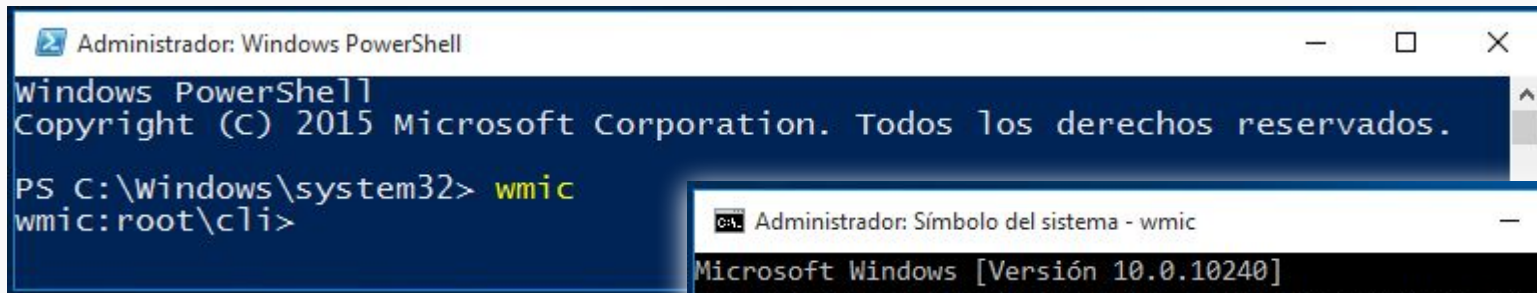
- Información básica del Sistema
- Servicios en uso
 - Red
 - Local
- Usuarios, grupos y contraseñas
- Protección de datos
- Seguridad del Sistema Operativo y Aplicaciones
- Auditoría y Logging

WMIC

- ¿Qué es WMIC? (Windows Management Instrumentation Command-Line)
 - ¿Sobre qué funciona?
 - ¿Dónde funciona?
 - ¿Qué permite ver?
- Generación de Reportes WMIC
- Auditoría con WMIC
 - Fundamentos de los Scripts de Auditoría

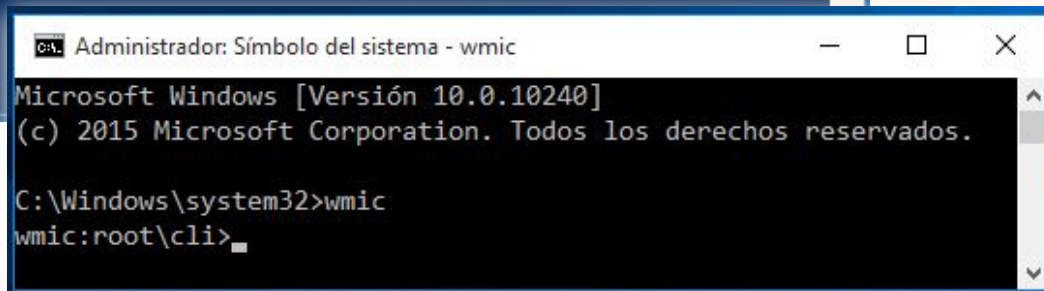
¿Dónde Funciona WMIC?

- Corre desde Windows XP/2003 en adelante
 - Abrir una terminal de comandos
 - Típear “wmic” y presionar enter
- Modos Interactivo y No-Interactivo
 - Nos interesa el No-Interactivo para automatizar los procesos de auditoría

A screenshot of a Windows PowerShell console window titled "Administrador: Windows PowerShell". The window has a dark blue background with white text. It shows the copyright notice for Microsoft Corporation (2015) and the current directory path C:\Windows\system32. The command "wmic" has been entered, and the prompt has changed to "wmic:root\cli>".

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Windows\system32> wmic
wmic:root\cli>
```

A screenshot of a Windows Command Prompt window titled "Administrador: Símbolo del sistema - wmic". The window has a black background with white text. It shows the version information for Microsoft Windows (10.0.10240) and the copyright notice for Microsoft Corporation (2015). The command "wmic" has been entered, and the prompt has changed to "wmic:root\cli>".

```
Administrador: Símbolo del sistema - wmic
Microsoft Windows [Versión 10.0.10240]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>wmic
wmic:root\cli>
```

¿Qué permite ver WMIC?

- Casi todo
 - Esencialmente expone casi cualquier configuración con el fin de solucionar problemas y automatizar
- Ejemplos:
 - Configuración de Red (NIC)
 - Configuraciones de Escritorio
 - Usuarios y Grupos
 - Estado de bloqueo de Contraseñas
 - Información de Configuración del Sistema
 - Logs de Eventos

Reportes de WMIC

- Esencialmente basados en texto
 - WMIC <objeto> <verbo>
- No siempre devuelve una salida elegante
 - Por lo general, inferior a 80 columnas
 - Se muestra en más espacio que el de la pantalla
- Existen otras opciones
 - La mayoría tienen una selección “breve”
 - Todas las opciones son visibles a través de:
 - WMIC <objeto> list /?

Auditoría Avanzada de Sistemas Windows

Objetivo de Auditoría: Identificar el Sistema

- **Objetivo:** obtener información básica del equipo siendo auditado
 - Tipo de Sistema Operativo
 - Versión: número de compilación, nivel de service pack, etc.
 - Información del Sistema: tiempo de actividad, usuario/compañía registrado, etc.
 - Hardware básico: CPU, memoria, disco
 - Las particiones deberían ser NTFS
- **Propósito:** identificar aspectos clave del equipo auditado

Información Básica del Sistema

- Herramienta de línea de comando
 - ver
 - systeminfo
- Herramienta con Interfaz gráfica
 - winver
 - msinfo32
- Herramientas de terceros
 - psinfo de Sysinternals



```
C:\Windows\system32>ver
```

```
Microsoft Windows [Versión 10.0.10240]
```

```
C:\Windows\system32>systeminfo
```

```
Nombre de host:                DESKTOP-9I91T7U
Nombre del sistema operativo:   Microsoft Windows 10 Pro
Versión del sistema operativo:  10.0.10240 N/D Compilación 10240
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
```

Preguntas a Hacer

- ¿El Sistema Operativo en uso está al día?
- ¿El Service Pack instalado es el último?
- ¿El Disco está formateado con NTFS?
- ¿Cuando fue parchado por última vez el equipo?
- ¿Hay alguna aplicación no autorizada instalada?

Herramienta: psinfo

```
C:\Users\vagrant\Desktop\PSTools>PsInfo.exe -h -s -d

PsInfo v1.78 - Local and remote system information viewer
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

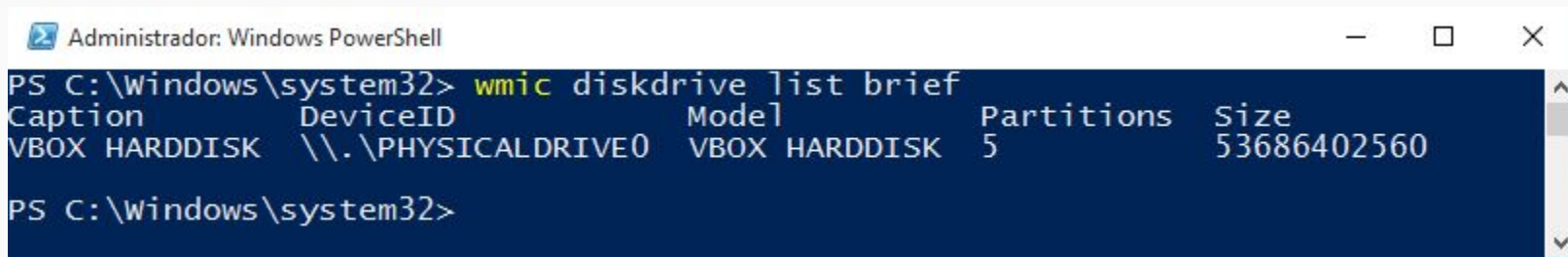
System information for \\WINDOWS-10-TEST:
Uptime:                        0 days 0 hours 9 minutes 38 seconds
Kernel version:                Windows 10 Enterprise Evaluation, Multiprocessor Free
Product type:                  Professional
Product version:               6.3
Service pack:                  0
Kernel build number:           18363
Registered organization:       Vagrant
Registered owner:              Vagrant
IE version:                    9.0000
System root:                   C:\Windows
Processors:                    2
Processor speed:               1.9 GHz
Processor type:                Intel(R) Core(TM) i7-8550U CPU @
Physical memory:               2 MB
Video driver:                  VirtualBox Graphics Adapter for Windows 8+
Volume Type      Format      Label      Size      Free      Free
      C: Fixed    NTFS      Windows 10 60.00 GB  37.74 GB  62.9%
      D: CD-ROM   CDFS      VBox_GAs_5.2.34 47.36 MB  0.0%
```

Installed HotFix
n/a Internet Explorer - 0

Applications:
Google Chrome 81.0.4044.138

WMIC - Discos

- Encontrar todos los dispositivos físicos
 - Podrían haber más dispositivos que los que están montados
- Encontrar todas las particiones lógicas y verificar el formato
 - No hay buenas razones para FAT32
- Comandos
 - `wmic diskdrive list brief`
 - `wmic logicaldisk list`



```
Administrador: Windows PowerShell
PS C:\windows\system32> wmic diskdrive list brief
Caption          DeviceID          Model             Partitions  Size
VBOX HARDDISK    \\.\PHYSICALDRIVE0 VBOX HARDDISK    5           53686402560
PS C:\windows\system32>
```

WMIC - Discos

```
<RESULTS NODE="DESKTOP-9I91T7U" >
<CIM>
  <INSTANCE CLASSNAME="Win32_LogicalDisk" >
    <PROPERTY NAME="Access" TYPE="uint16" >
      <VALUE>0</VALUE>
    </PROPERTY>
    <PROPERTY NAME="Availability" PROPAGATED="true" TYPE="uint16" />
    <PROPERTY NAME="BlockSize" PROPAGATED="true" TYPE="uint64" />
    <PROPERTY NAME="Caption" TYPE="string" >
      <VALUE>C:</VALUE>
    </PROPERTY>
    <PROPERTY NAME="Compressed" TYPE="boolean" >
```

Administrador: Windows PowerShell

```
PS C:\Windows\system32> wmic logicaldisk list /format:xml > C:\logicaldisk.html
PS C:\Windows\system32>
```

```
    <VALUE>Disco fijo local</VALUE>
  </PROPERTY>
  <PROPERTY NAME="DeviceID" TYPE="string" >
    <VALUE>C:</VALUE>
  </PROPERTY>
  <PROPERTY NAME="DriveType" TYPE="uint32" >
    <VALUE>3</VALUE>
  </PROPERTY>
  <PROPERTY NAME="ErrorCleared" PROPAGATED="true" TYPE="boolean" />
  <PROPERTY NAME="ErrorDescription" PROPAGATED="true" TYPE="string" />
  <PROPERTY NAME="ErrorMethodology" PROPAGATED="true" TYPE="string" />
  <PROPERTY NAME="FileSystem" TYPE="string" >
    <VALUE>NTFS</VALUE>
  </PROPERTY>
```

Parches/Actualizaciones del Sistema Operativo

- **Objetivo:** asegurar que el sistema está actualizado con los parches de seguridad críticos
- **Propósito:** las actualizaciones de sistema y parches de seguridad protegen al equipo de ser comprometido
 - Muchos compromisos ocurren a través de vulnerabilidades conocidas que nunca fueron arregladas
 - El parchado es una de las maneras más fáciles de abordar este problema
 - El software no soportado puede ser “no parchable” y vulnerable por defecto

Herramientas de Auditoría: Estado de Parches

- Microsoft Baseline Security Analyzer (MBSA)
- Herramientas de Administración de Parches
 - Microsoft SUS / WUS / SMS
 - Herramientas de Administración de Parches de terceros

Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer 2.1

Microsoft
Baseline Security Analyzer

Report Details for WORKGROUP - WINDOWS-10-TEST (2020-05-13 10:08:03)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: WORKGROUP\WORKGROUP-10-TEST
IP address: 127.0.0.1
Security report name: WORKGROUP - WINDOWS-10-TEST
Scan date: 5/13/2020 10:08:03
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date: 5/13/2020 10:08:03
Security update catalog: Windows Server 2016

Sort Order:

Security Update Scan Results

Score	Issue	Result
!	Security Updates	An error occurred while scanning for updates. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (3 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✗	Automatic Updates	The Automatic Updates system service is not configured to be started as Automatic. What was scanned How to correct this
✗	Autologon	Autologon is configured on this computer. What was scanned How to correct this
!	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
✓	Windows Firewall	Windows Firewall is enabled on all network connections. What was scanned Result details

Tipos de Parches de Windows

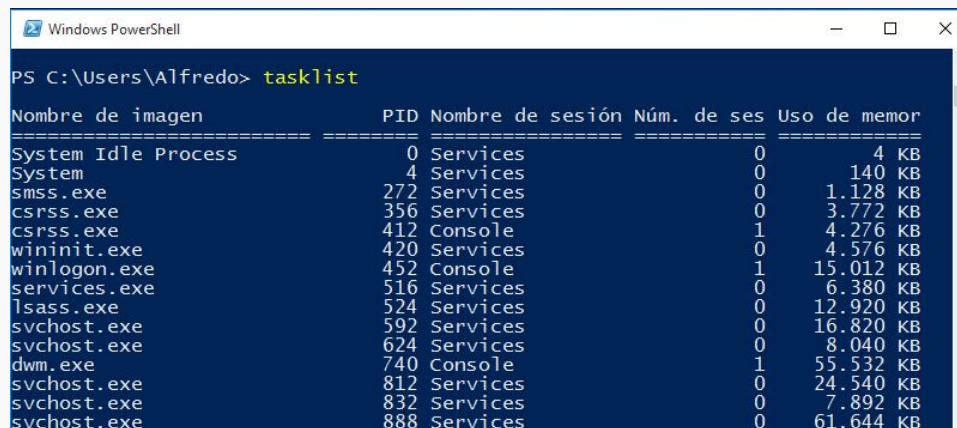
- Service Packs
 - Actualizaciones importantes que reúnen parches previos de seguridad y generales. Pueden incluir nuevas características.
- Actualizaciones Críticas o Hotfixes
 - Reparación para un problema crítico simple que afecta la seguridad o estabilidad del sistema
- Reparaciones QFE (Quick Fix Engineering)
 - Reparación para un problema específico simple, generalmente disponible solamente a través de Microsoft Support

Preguntas Adicionales de Auditoría

- ¿Política de Control de Cambios?
 - ¿Cuántas pruebas se eligen/requieren antes de desplegar los parches?
- ¿Mantenimiento programado?
 - ¿Se tiene regularmente un mantenimiento programado? ¿Qué tan seguido ocurre?
- ¿Política de Cumplimiento?
 - ¿La organización requiere instalar ciertos parches o cumplir con un nivel de parches en particular? ¿Se está cumpliendo con esta política?
- ¿Política de Excepción?
 - ¿Cuándo es correcto no parchar?

Componentes/Servicios Innecesarios

- Asegurar que solamente las características necesarias del Sistema Operativo están instaladas/corriendo
- Herramientas de Auditoría:
 - nmap
 - fport / openports
 - psservice / scquery / tasklist



Windows PowerShell

```
PS C:\Users\Alfredo> tasklist
```

Nombre de imagen	PID	Nombre de sesión	Núm. de ses	Uso de memor
System Idle Process	0	Services	0	4 KB
System	4	Services	0	140 KB
smss.exe	272	Services	0	1.128 KB
csrss.exe	356	Services	0	3.772 KB
csrss.exe	412	Console	1	4.276 KB
wininit.exe	420	Services	0	4.576 KB
winlogon.exe	452	Console	1	15.012 KB
services.exe	516	Services	0	6.380 KB
lsass.exe	524	Services	0	12.920 KB
svchost.exe	592	Services	0	16.820 KB
svchost.exe	624	Services	0	8.040 KB
dwm.exe	740	Console	1	55.532 KB
svchost.exe	812	Services	0	24.540 KB
svchost.exe	832	Services	0	7.892 KB
svchost.exe	888	Services	0	61.644 KB

Componentes/Servicios

- La instalación por defecto de cualquier SO es generalmente insegura
 - El vendedor (o administrador) puede instalar características para facilitar el uso.
- “Componentes” seleccionados/no seleccionados durante o luego de la instalación
 - Pueden ser instalados/desinstalados
 - Ejemplo: IIS, SNMP, Servicios de Impresión TCP/IP...
- “Servicios” pueden ser instalados como parte de componentes o ser contruidos dentro del SO
 - Solamente algunos pueden ser desinstalados (remove componente)
 - Pueden ser iniciados / detenidos / deshabilitados

Servicios Innecesarios

- Muchos servicios instalados por defecto no son requeridos para la operación
 - Ejemplo: IIS, SMTP, etc.
- Los servicios pueden contener vulnerabilidades
- Servicios no utilizados:
 - Probablemente no serán parchados
 - Deberían ser removidos o deshabilitados
- Falsos servicios pueden indicar infección de malware

¿Cómo verificar los Servicios?

- Servicios escuchando (puertos abiertos):
 - “Desde afuera”: desde un equipo externo (escaneo de puertos)
 - “Desde adentro”: desde el mismo equipo (netstat, openports)
- Es bueno hacer ambos y correlacionar resultados
 - El escaneo desde afuera puede ser más confiable
 - Los servicios locales pueden no ser visibles para los externos
- Lista completa de servicios
 - MMC para Servicios
 - Psservice.exe, tasklist
 - WMIC (service list brief)

WMIC: service list brief

Windows PowerShell

```
PS C:\Users\Alfredo> wmic service list brief
```

ExitCode	Name	ProcessId	StartMode	State	Status
1077	AJRouter	0	Manual	Stopped	OK
1077	ALG	0	Manual	Stopped	OK
1077	AppIDSvc	0	Manual	Stopped	OK
1077	Appinfo	0	Manual	Stopped	OK
1077	AppMgmt	0	Manual	Stopped	OK
0	AppReadiness	0	Manual	Stopped	OK
0	AppXSvc	0	Manual	Stopped	OK
0	AudioEndpointBuilder	888	Auto	Running	OK
0	Audiosrv	812	Auto	Running	OK
1077	AxInstSV	0	Manual	Stopped	OK
1077	BDESVC	0	Manual	Stopped	OK
0	BFE	1184	Auto	Running	OK
0	BITS	964	Auto	Running	OK
0	BrokerInfrastructure	592	Auto	Running	OK
1077	Browser	0	Manual	Stopped	OK
1077	BthHFSrv	0	Manual	Stopped	OK
1077	bthserv	0	Manual	Stopped	OK
1077	CDPSvc	0	Manual	Stopped	OK
1077	CertPropSvc	0	Manual	Stopped	OK
0	ClipSVC	1576	Manual	Running	OK
1077	COMSysApp	0	Manual	Stopped	OK
0	CoreMessagingRegistrar	1184	Auto	Running	OK
0	CryptSvc	1056	Auto	Running	OK
1077	CscService	0	Manual	Stopped	OK
0	DcomLaunch	592	Auto	Running	OK

Preguntas Adicionales de Auditoría

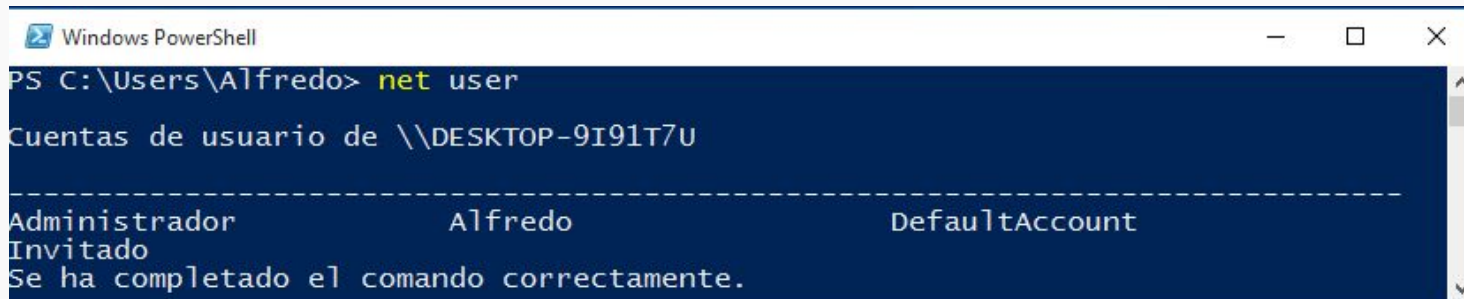
- ¿Existen procesos o estándares de instalación o configuración para sistemas Windows?
- ¿Hay alguna política que describa los servicios permitidos o prohibidos?
- ¿Están los administradores de sistemas familiarizados con los servicios y puertos estándares que deberían estar presentes en sus sistemas?
- ¿Se realizan verificaciones periódicas para detectar puertos o servicios nuevos o cambiados?

Problemas con Usuarios y Grupos

- Solamente Usuarios válidos en el Sistema
- Los Grupos tienen membresías apropiadas
- Sin contraseñas en blanco
- Política de Contraseñas apropiada
- Contraseñas “fuertes” en uso
- Cuentas Locales vs. Cuentas de Dominio

Usuarios Válidos

- **Objetivo:** Usuarios Autorizados
 - Asegurar que solamente cuentas de usuario válidas y activas están presentes
- **Actividades de Auditoría:**
 - Net user
 - Addusers
 - DumpSec (Somarsoft)
 - Consultas a Active Directory



```
Windows PowerShell
PS C:\Users\Alfredo> net user

Cuentas de usuario de \\DESKTOP-9I91T7U

-----
Administrador          Alfredo              DefaultAccount
Invitado
Se ha completado el comando correctamente.
```

Cuentas de Usuario “Huérfanas”

- Cuentas no utilizadas que permanecen en el sistema
 - El usuario deja la organización
 - El usuario tiene una cuenta que nunca usa
- Encontrar:
 - Cuentas no utilizadas > 30 días
 - Cuentas que nunca iniciaron sesión
- Verificar con el usuario o sus gerentes para ver si la cuenta es necesaria
- Deshabilitar o borrar cuentas innecesarias

Otros Problemas con Cuentas

- Uso de fecha de expiración
- Limitar horarios de login
- Cuentas especiales
 - Administrador / Invitado
 - Cuentas incorporadas
 - IUSR/IWAM, TSInternetUser
 - HelpAssistant, SUPPORT

Cuentas de Servicio

- Los servicios deben correr en el contexto de una cuenta de usuario
- Si el servicio es comprometido, el atacante tiene privilegios del servicio
- Muchos servicios corren como SYSTEM/LocalSystem o Local Service/Network Service
- Muchas aplicaciones corren con acceso Administrador o Administrador de Dominio por defecto
- Deberían correr con mínimos privilegios requeridos
- Verificar cuentas usadas por varios servicios

Grupos Apropriados

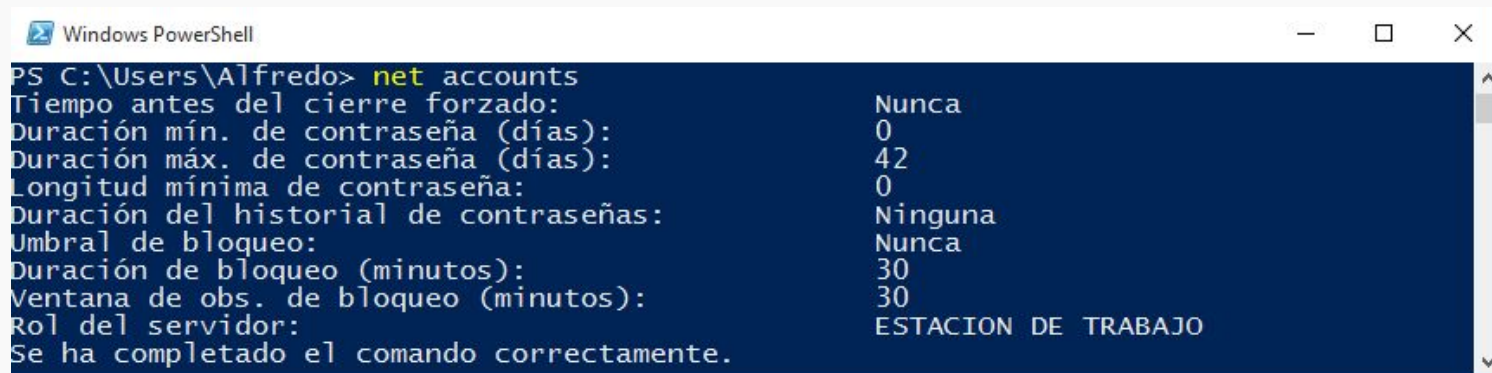
- **Objetivo:** Membresías de Grupo son apropiadas y hacen cumplir el Mínimo Privilegio
- **Actividades de Auditoría:**
 - dsquery
 - DumpSec (Somarsoft)

Membresías de Grupo

- Los Grupos se utilizan para conceder permisos y privilegios
- Las membresías restringen (o conceden) acceso a recursos
- Los grupos sensibles deberían ser monitoreados
- Los grupos de Administrador deberían tener muy poca gente

Contraseñas Fuertes

- **Objetivo:** Las Contraseñas son administradas de manera apropiada
 - Las contraseñas están en uso, son “fuertes”, están administradas con una buena política, están protegidas por cifrado fuerte
- **Actividades de Auditoría**
 - net accounts, DumpSec.
 - Herramientas de Evaluación de Contraseñas.
 - Verificación de Registro/Configuraciones.



```
Windows PowerShell
PS C:\Users\Alfredo> net accounts
Tiempo antes del cierre forzado:          Nunca
Duración mín. de contraseña (días):       0
Duración máx. de contraseña (días):       42
Longitud mínima de contraseña:            0
Duración del historial de contraseñas:     Ninguna
Umbral de bloqueo:                        Nunca
Duración de bloqueo (minutos):             30
Ventana de obs. de bloqueo (minutos):     30
Rol del servidor:                         ESTACION DE TRABAJO
Se ha completado el comando correctamente.
```

Requerimientos de Autenticación

- El acceso a sistemas debería ser restringido/controlado
- Windows requiere usuario/contraseña
 - Pero la contraseña puede estar vacía o ser débil
- Problemas clave de Auditoría son:
 - Existencia de Contraseñas
 - Cambios de contraseña frecuente requeridos
 - Cumplimiento del uso de Contraseñas “fuertes”
 - Utilización de buen cifrado para proteger Contraseñas

Preguntas Adicionales de Auditoría

- Administración de Cuentas de Usuario
 - ¿Quién solicita cuentas? ¿Quién puede crear cuentas? ¿Cómo se notifica sobre empleados que se van de la compañía?
- Administración de Grupos
 - ¿Quién determina los miembros de los grupos? ¿Quién revisa las membresías?
- Contraseñas
 - ¿Existe política abordando contraseñas o autenticación? ¿Son evaluadas regularmente las contraseñas? ¿Quién está autorizado a hacer esto?

¿Qué más debe auditarse?

- Acceso restringido a Recursos
 - Mínimos Privilegios / Necesidad de Saber
 - Datos almacenados (archivos con información sensible)
 - Privilegios y Permisos (objetos NTFS) en Windows
- Integridad de Archivos
 - Asegurar que archivos claves no han sido modificados o manipulados (hashes)
- Información en Tránsito
 - Privacidad, cifrado, integridad, autenticidad en la comunicación
- Vulnerabilidades Específicas del Sistema Operativo
- Pistas de Auditoría (Logging, Visor de Eventos)

¿Preguntas?

¡Muchas Gracias!