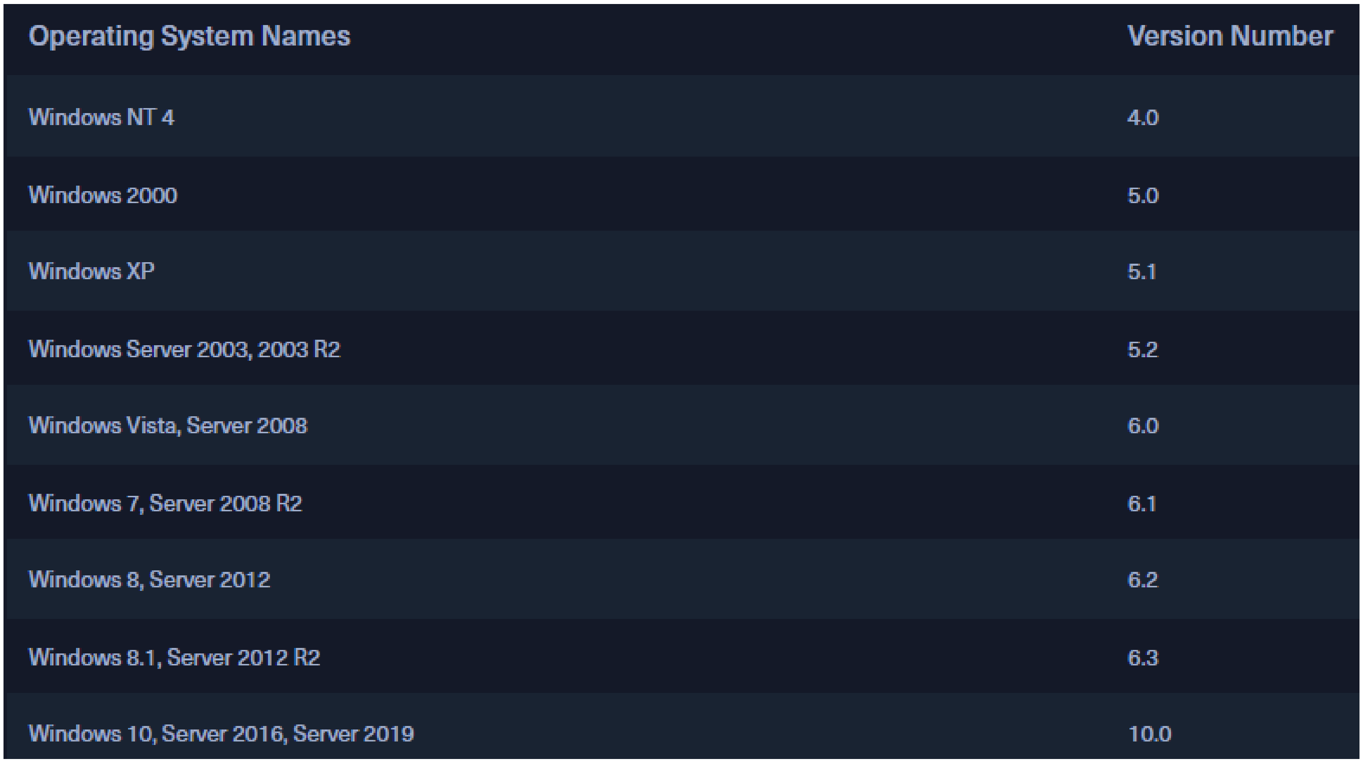
Windows Fundamentals (intro)

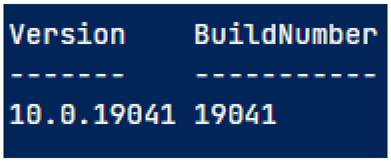
Windows Versions



Operating System Names	Version Number
Windows NT 4	4.0
Windows 2000	5.0
Windows XP	5.1
Windows Server 2003, 2003 R2	5.2
Windows Vista, Server 2008	6.0
Windows 7, Server 2008 R2	6.1
Windows 8, Server 2012	6.2
Windows 8.1, Server 2012 R2	6.3
Windows 10, Server 2016, Server 2019	10.0

Para obtener información sobre el Sistema Operativo (O.S) podemos introducir el siguiente comando en la PowerShell:

```
Get-WmiObject -Class win32_OperatingSystem
```



```
Version    BuildNumber
-------    -----------
10.0.19041 19041
```

También podemos listar procesos con `Win32_Process` ,listar servicios con `Win32_Service` o información de la propia BIOS con `Win32_Bios`.

Remote Desktop Protocol (RDP)

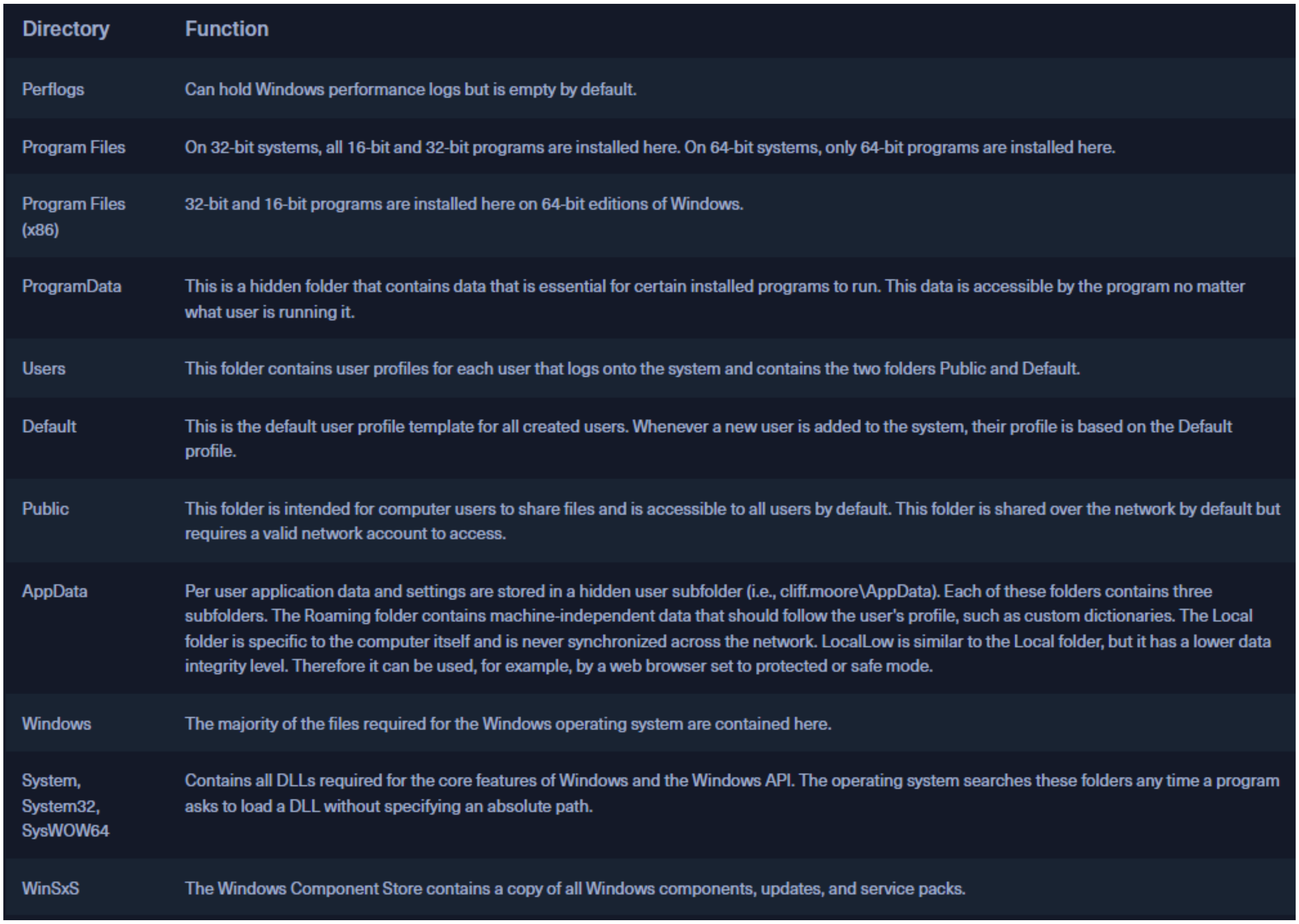
Es importante tener en cuenta que RDP escucha de forma predeterminada en el puerto lógico 3389.

En caso de que nos queremos conectar entre máquinas Windows se dispone de una herramienta nativa que nos permite realizar este proceso de conexión.

En entornos Linux con herramientas como **xfreerdp** se nos permite aprovechar este protocolo para conectarnos de forma remota desde nuestra máquina Linux a una máquina Windows.

Operating System Structure

Estos son los diferentes directorios con sus respectivas funciones:



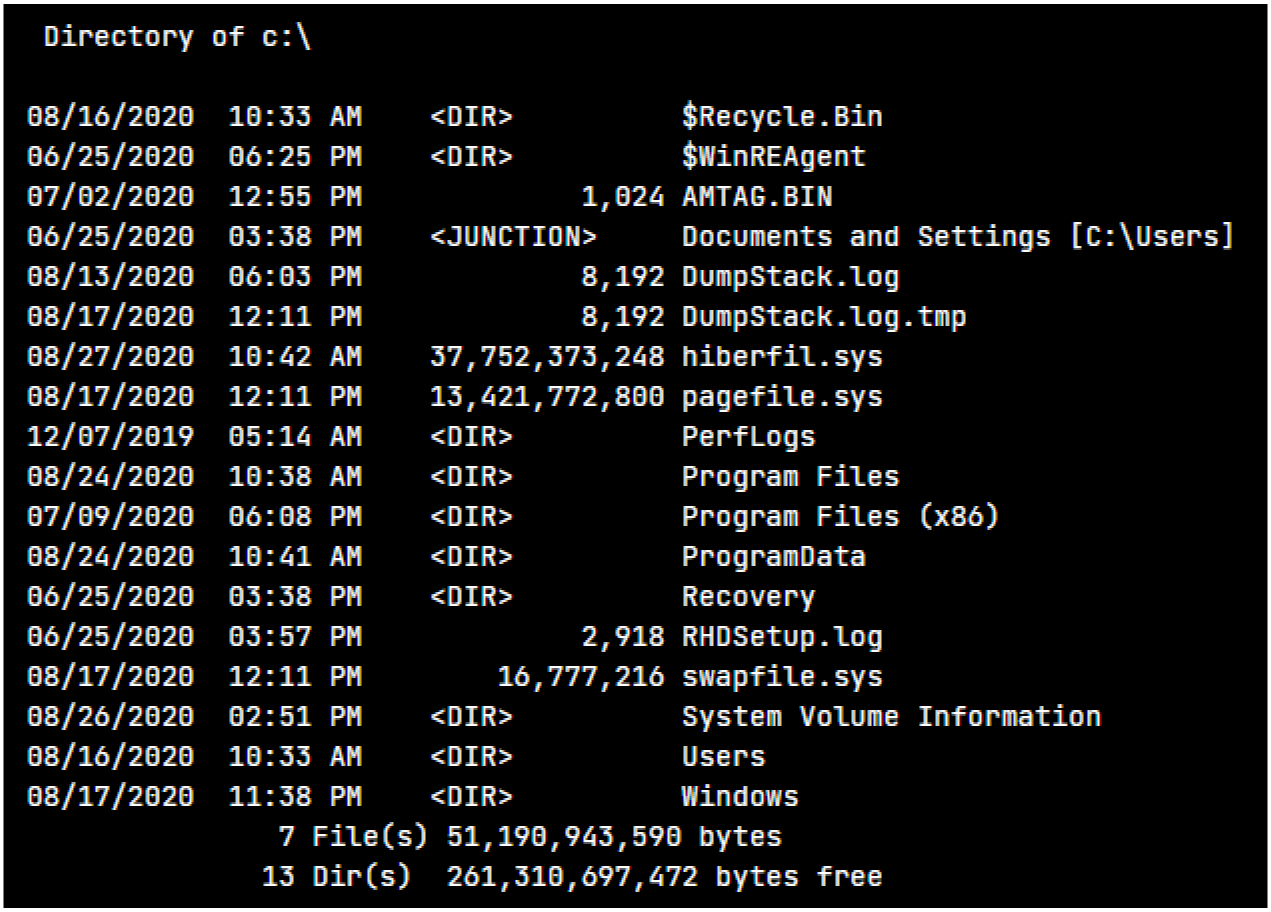
Directory	Function
Perflogs	Can hold Windows performance logs but is empty by default.
Program Files	On 32-bit systems, all 16-bit and 32-bit programs are installed here. On 64-bit systems, only 64-bit programs are installed here.
Program Files (x86)	32-bit and 16-bit programs are installed here on 64-bit editions of Windows.
ProgramData	This is a hidden folder that contains data that is essential for certain installed programs to run. This data is accessible by the program no matter what user is running it.
Users	This folder contains user profiles for each user that logs onto the system and contains the two folders Public and Default.
Default	This is the default user profile template for all created users. Whenever a new user is added to the system, their profile is based on the Default profile.
Public	This folder is intended for computer users to share files and is accessible to all users by default. This folder is shared over the network by default but requires a valid network account to access.
AppData	Per user application data and settings are stored in a hidden user subfolder (i.e., cliff.moore\AppData). Each of these folders contains three subfolders. The Roaming folder contains machine-independent data that should follow the user's profile, such as custom dictionaries. The Local folder is specific to the computer itself and is never synchronized across the network. LocalLow is similar to the Local folder, but it has a lower data integrity level. Therefore it can be used, for example, by a web browser set to protected or safe mode.
Windows	The majority of the files required for the Windows operating system are contained here.
System, System32, SysWOW64	Contains all DLLs required for the core features of Windows and the Windows API. The operating system searches these folders any time a program asks to load a DLL without specifying an absolute path.
WinSxS	The Windows Component Store contains a copy of all Windows components, updates, and service packs.

Exploring Directories Using Command Line

Con el siguiente comando se nos permite movernos entre directorios:

```
dir <ruta>
```

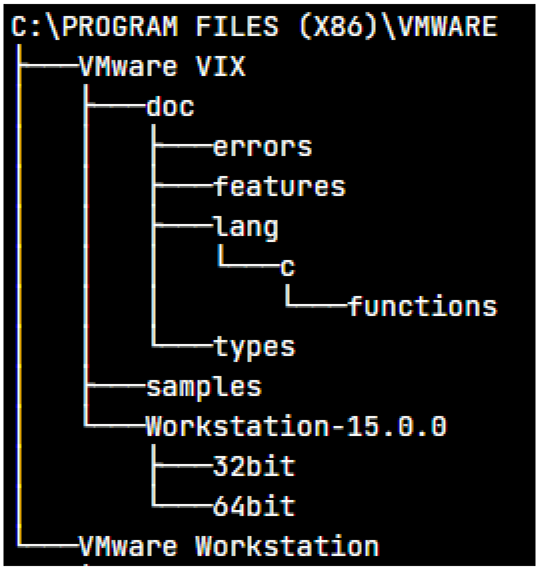
Si quisiéramos ver el contenido de `c:\` veríamos algo como:



```
 Directory of c:\

08/16/2020  10:33 AM    <DIR>          $Recycle.Bin
06/25/2020  06:25 PM    <DIR>          $WinREAgent
07/02/2020  12:55 PM             1,024 AMTAG.BIN
06/25/2020  03:38 PM    <JUNCTION>     Documents and Settings [C:\Users]
08/13/2020  06:03 PM             8,192 DumpStack.log
08/17/2020  12:11 PM             8,192 DumpStack.log.tmp
08/27/2020  10:42 AM    37,752,373,248 hiberfil.sys
08/17/2020  12:11 PM    13,421,772,800 pagefile.sys
12/07/2019  05:14 AM    <DIR>          PerfLogs
08/24/2020  10:38 AM    <DIR>          Program Files
07/09/2020  06:08 PM    <DIR>          Program Files (x86)
08/24/2020  10:41 AM    <DIR>          ProgramData
06/25/2020  03:38 PM    <DIR>          Recovery
06/25/2020  03:57 PM             2,918 RHDSetup.log
08/17/2020  12:11 PM        16,777,216 swapfile.sys
08/26/2020  02:51 PM    <DIR>          System Volume Information
08/16/2020  10:33 AM    <DIR>          Users
08/17/2020  11:38 PM    <DIR>          Windows
               7 File(s) 51,190,943,590 bytes
              13 Dir(s)  261,310,697,472 bytes free
```

Para tener una visión global podemos usar el comando `tree`:

```
tree <ruta>
```

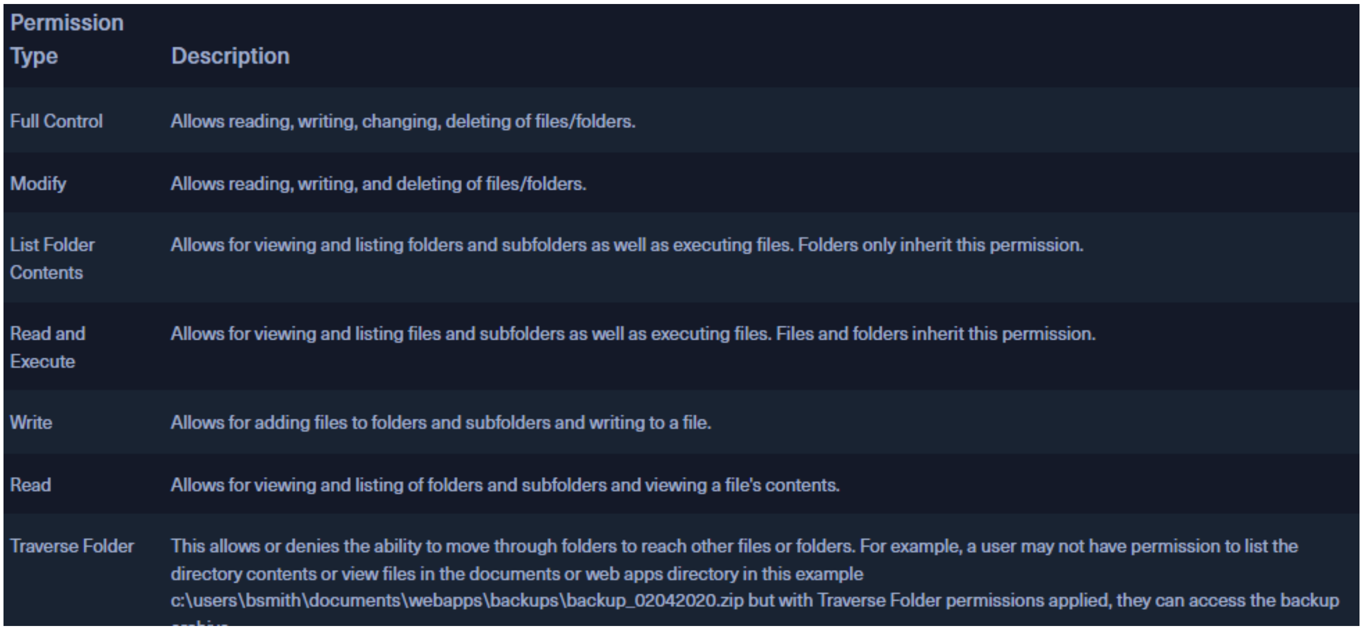


```
C:\PROGRAM FILES (X86)\VMWARE
├───VMware VIX
│   ├───doc
│   │   ├───errors
│   │   ├───features
│   │   ├───lang
│   │   │   └───c
│   │   │       └───functions
│   │   └───types
│   ├───samples
│   └───Workstation-15.0.0
│       ├───32bit
│       └───64bit
└───VMware Workstation
```

File System

Existen cinco tipos de sistemas de archivos de Windows: **FAT12, FAT16, FAT32, NTFS y exFAT**. FAT12 y FAT16 ya no se utilizan en los sistemas operativos Windows modernos. En esta capacitación, abordaremos los sistemas de archivos FAT32 y exFAT, pero nos centraremos principalmente en el sistema de archivos **NTFS**.

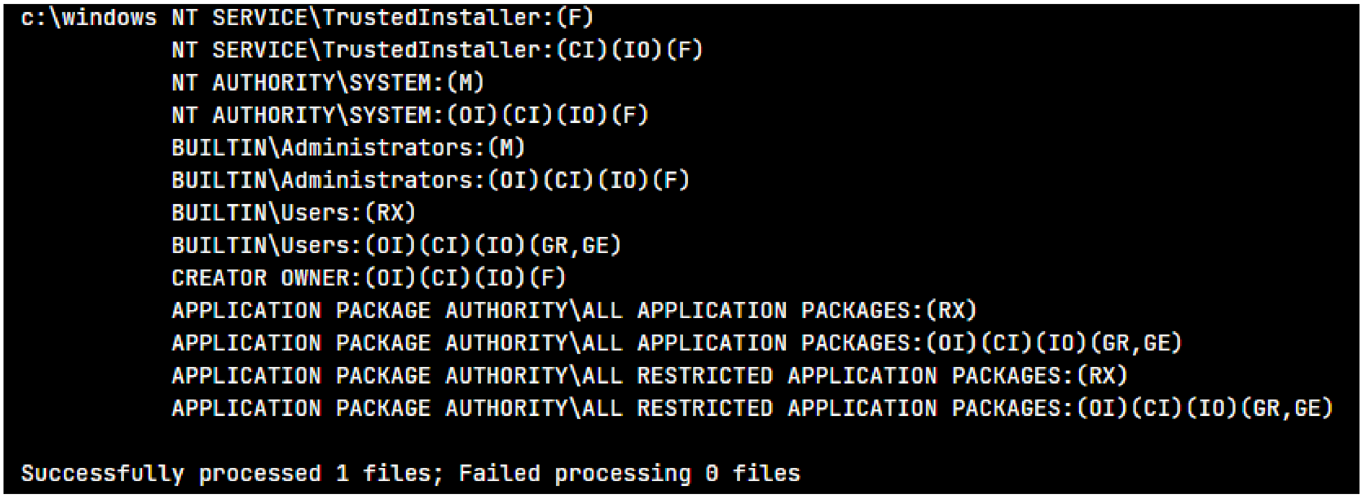
Permissions



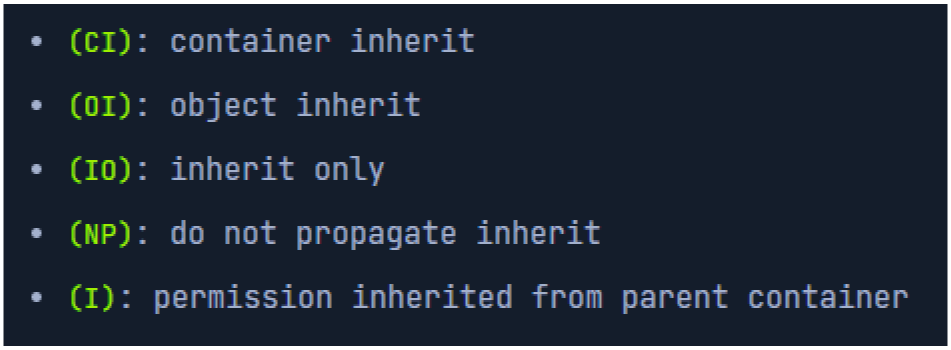
Permission Type	Description
Full Control	Allows reading, writing, changing, deleting of files/folders.
Modify	Allows reading, writing, and deleting of files/folders.
List Folder Contents	Allows for viewing and listing folders and subfolders as well as executing files. Folders only inherit this permission.
Read and Execute	Allows for viewing and listing files and subfolders as well as executing files. Files and folders inherit this permission.
Write	Allows for adding files to folders and subfolders and writing to a file.
Read	Allows for viewing and listing of folders and subfolders and viewing a file's contents.
Traverse Folder	This allows or denies the ability to move through folders to reach other files or folders. For example, a user may not have permission to list the directory contents or view files in the documents or web apps directory in this example c:\users\bsmith\documents\webapps\backups\backup_02042020.zip but with Traverse Folder permissions applied, they can access the backup

Integrity Control Access Control List (icacls)

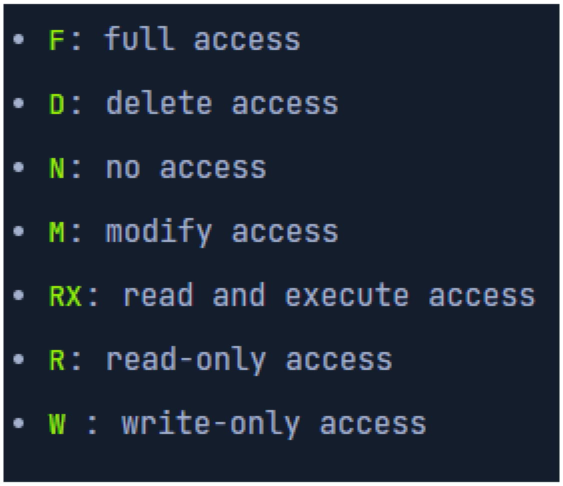
```
icacls c:\windows
```



```
c:\windows NT SERVICE\TrustedInstaller:(F)
           NT SERVICE\TrustedInstaller:(CI)(IO)(F)
           NT AUTHORITY\SYSTEM:(M)
           NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
           BUILTIN\Administrators:(M)
           BUILTIN\Administrators:(OI)(CI)(IO)(F)
           BUILTIN\Users:(RX)
           BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
           CREATOR OWNER:(OI)(CI)(IO)(F)
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```

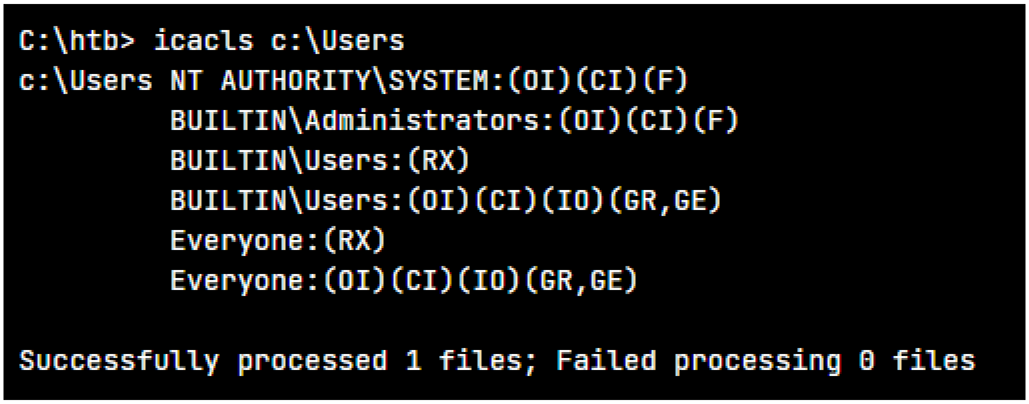


- (CI): container inherit
- (OI): object inherit
- (IO): inherit only
- (NP): do not propagate inherit
- (I): permission inherited from parent container

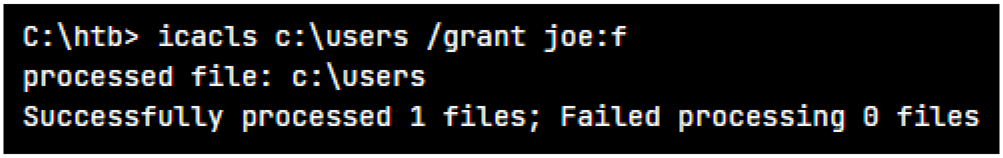


- F: full access
- D: delete access
- N: no access
- M: modify access
- RX: read and execute access
- R: read-only access
- W : write-only access

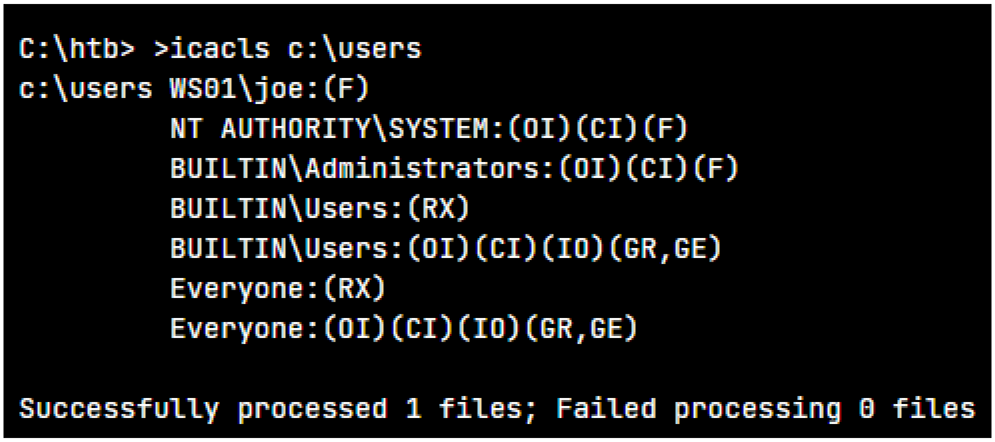
Podemos agregar y eliminar permisos mediante la línea de comandos usando **icacls**. Aquí, ejecutamos icacls en el contexto de una cuenta de administrador local que muestra el directorio C:\users, donde el usuario joe no tiene permisos de escritura.



```
C:\htb> icacls c:\Users
c:\Users NT AUTHORITY\SYSTEM:(OI)(CI)(F)
         BUILTIN\Administrators:(OI)(CI)(F)
         BUILTIN\Users:(RX)
         BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
         Everyone:(RX)
         Everyone:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```



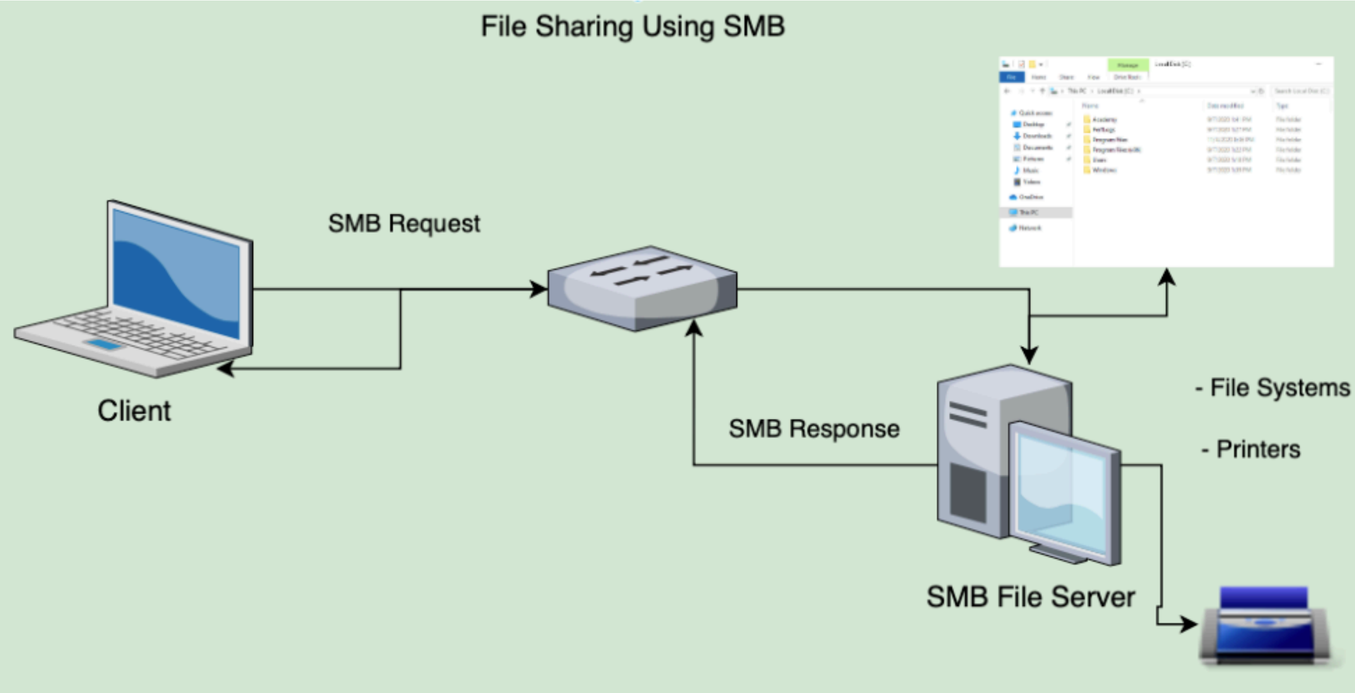
```
C:\htb> icacls c:\users /grant joe:f
processed file: c:\users
Successfully processed 1 files; Failed processing 0 files
```



```
C:\htb> >icacls c:\users
c:\users WS01\joe:(F)
         NT AUTHORITY\SYSTEM:(OI)(CI)(F)
         BUILTIN\Administrators:(OI)(CI)(F)
         BUILTIN\Users:(RX)
         BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
         Everyone:(RX)
         Everyone:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```

NTFS vs. Share Permissions

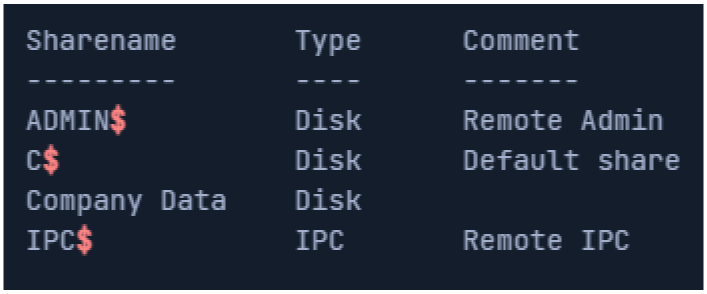
El protocolo de bloque de mensajes del servidor (**SMB**) se utiliza en Windows para conectar recursos compartidos, como archivos e impresoras. Se utiliza en entornos empresariales grandes, medianos y pequeños. Vea la imagen a continuación para visualizar este concepto:



Son carpetas compartidas en las que los usuarios externos pueden acceder al contenido siempre que tengan permisos para ello:

En este caso tenemos la carpeta compartido **Company Data**:

```
smbclient -L SERVER_IP -U htb-student
```

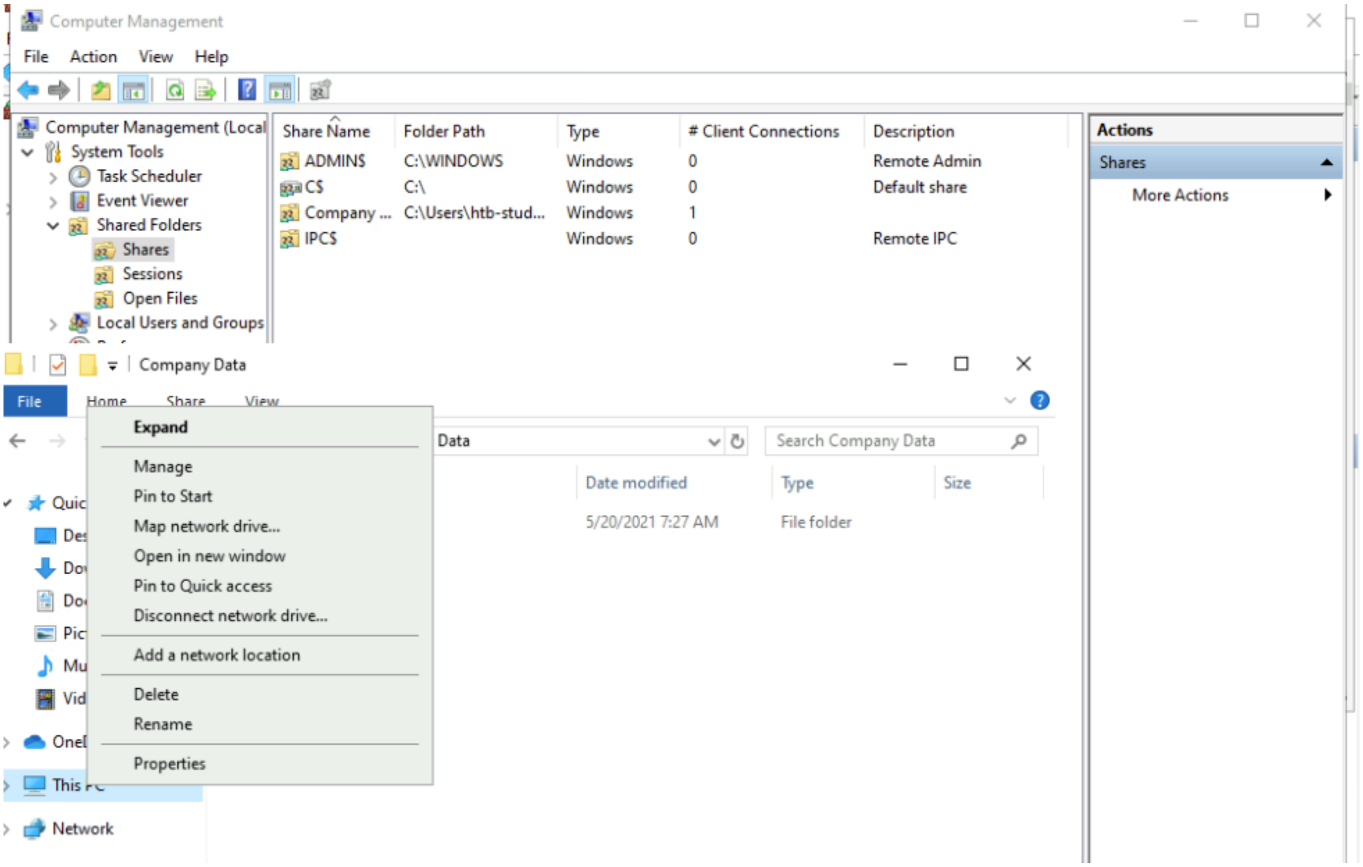


```
Sharename       Type      Comment
---------       ----      -------
ADMIN$          Disk      Remote Admin
C$              Disk      Default share
Company Data    Disk
IPC$            IPC       Remote IPC
```

Para acceder a ella:

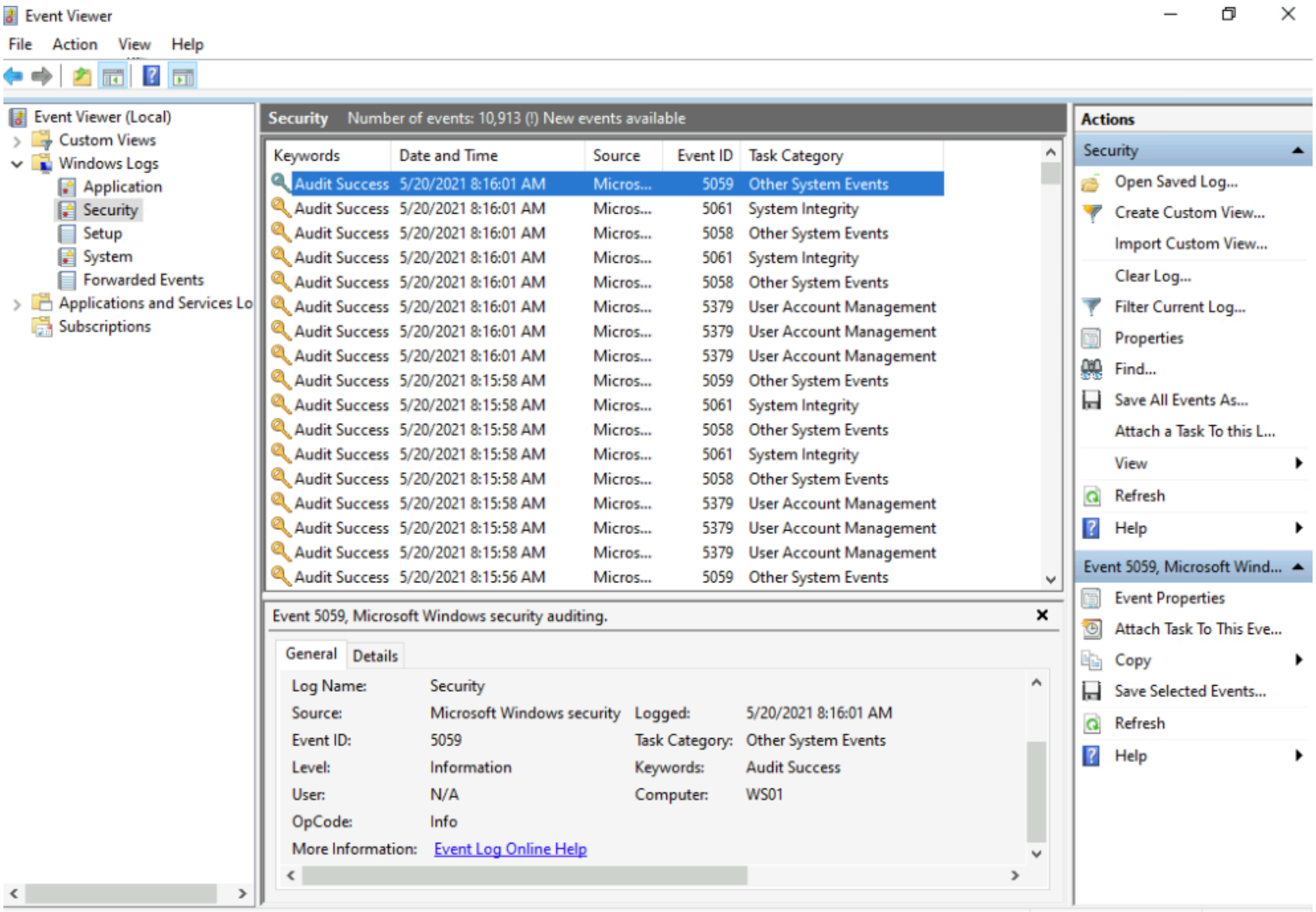
```
smbclient '\\SERVER_IP\Company Data' -U htb-student
```

Podemos adoptar medidas de seguridad como ACLs y ver los logs Events que esten sucediendo en la carpeta:



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\WINDOWS	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
Company ...	C:\Users\htb-stud...	Windows	1	
IPC$		Windows	0	Remote IPC

Date modified	Type	Size
5/20/2021 7:27 AM	File folder	



Security Number of events: 10,913 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/20/2021 8:16:01 AM	Micros...	5059	Other System Events
Audit Success	5/20/2021 8:16:01 AM	Micros...	5061	System Integrity
Audit Success	5/20/2021 8:16:01 AM	Micros...	5058	Other System Events
Audit Success	5/20/2021 8:16:01 AM	Micros...	5061	System Integrity
Audit Success	5/20/2021 8:16:01 AM	Micros...	5058	Other System Events
Audit Success	5/20/2021 8:16:01 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:16:01 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:16:01 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:15:58 AM	Micros...	5059	Other System Events
Audit Success	5/20/2021 8:15:58 AM	Micros...	5061	System Integrity
Audit Success	5/20/2021 8:15:58 AM	Micros...	5058	Other System Events
Audit Success	5/20/2021 8:15:58 AM	Micros...	5061	System Integrity
Audit Success	5/20/2021 8:15:58 AM	Micros...	5058	Other System Events
Audit Success	5/20/2021 8:15:58 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:15:58 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:15:58 AM	Micros...	5379	User Account Management
Audit Success	5/20/2021 8:15:56 AM	Micros...	5059	Other System Events

Event 5059, Microsoft Windows security auditing.

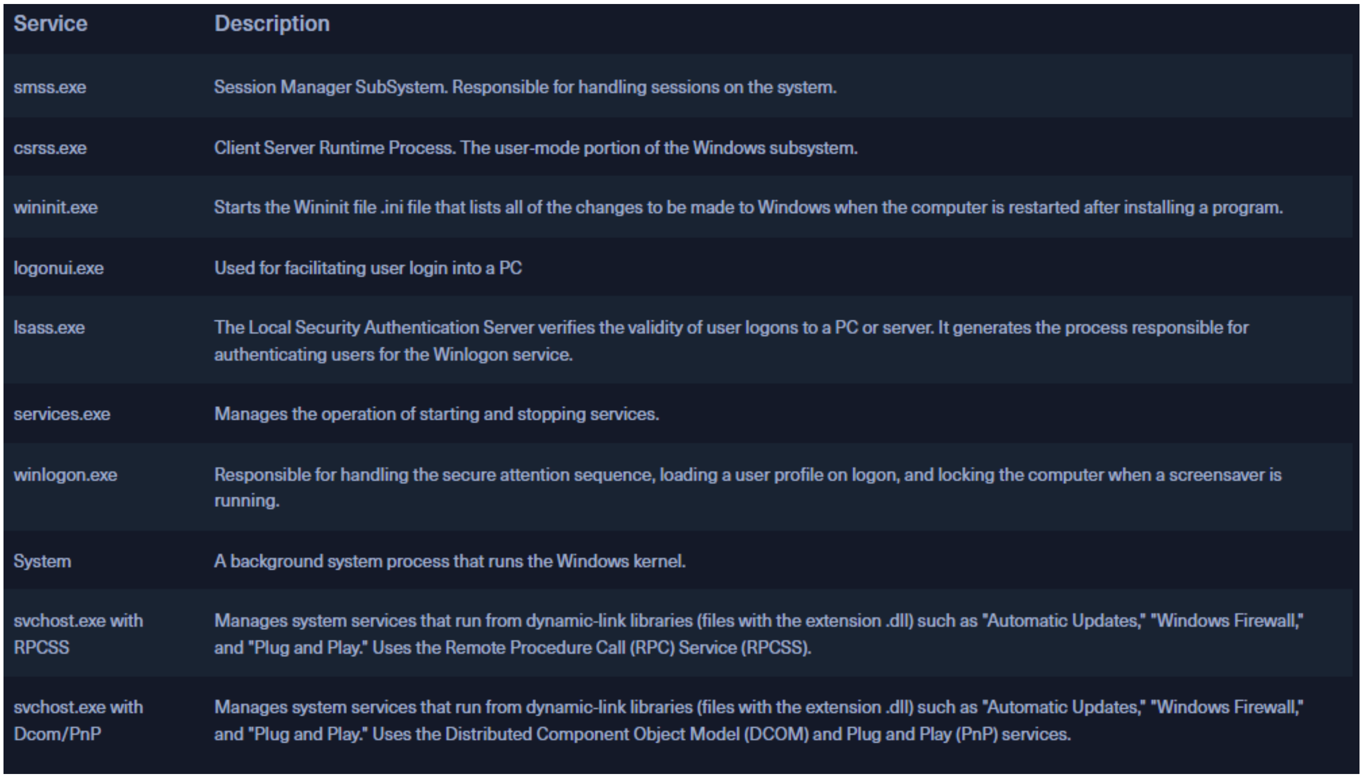
Log Name: Security
Source: Microsoft Windows security
Logged: 5/20/2021 8:16:01 AM
Event ID: 5059
Task Category: Other System Events
Level: Information
Keywords: Audit Success
User: N/A
Computer: WS01
OpCode: Info
More Information: Event Log Online Help

Windows Services & Processes

Si queremos ver que servicios están corriendo ahora mismo en nuestro Windows debemos ejecutar el siguiente comando:

```
Get-Service | ? {$_.Status -eq "Running"}
```

Algunos de los **servicios críticos** del sistema son:



Service	Description
smss.exe	Session Manager SubSystem. Responsible for handling sessions on the system.
csrss.exe	Client Server Runtime Process. The user-mode portion of the Windows subsystem.
wininit.exe	Starts the Wininit file .ini file that lists all of the changes to be made to Windows when the computer is restarted after installing a program.
logonui.exe	Used for facilitating user login into a PC
lsass.exe	The Local Security Authentication Server verifies the validity of user logons to a PC or server. It generates the process responsible for authenticating users for the Winlogon service.
services.exe	Manages the operation of starting and stopping services.
winlogon.exe	Responsible for handling the secure attention sequence, loading a user profile on logon, and locking the computer when a screensaver is running.
System	A background system process that runs the Windows kernel.
svchost.exe with RPCSS	Manages system services that run from dynamic-link libraries (files with the extension .dll) such as "Automatic Updates," "Windows Firewall," and "Plug and Play." Uses the Remote Procedure Call (RPC) Service (RPCSS).
svchost.exe with Dcom/PnP	Manages system services that run from dynamic-link libraries (files with the extension .dll) such as "Automatic Updates," "Windows Firewall," and "Plug and Play." Uses the Distributed Component Object Model (DCOM) and Plug and Play (PnP) services.

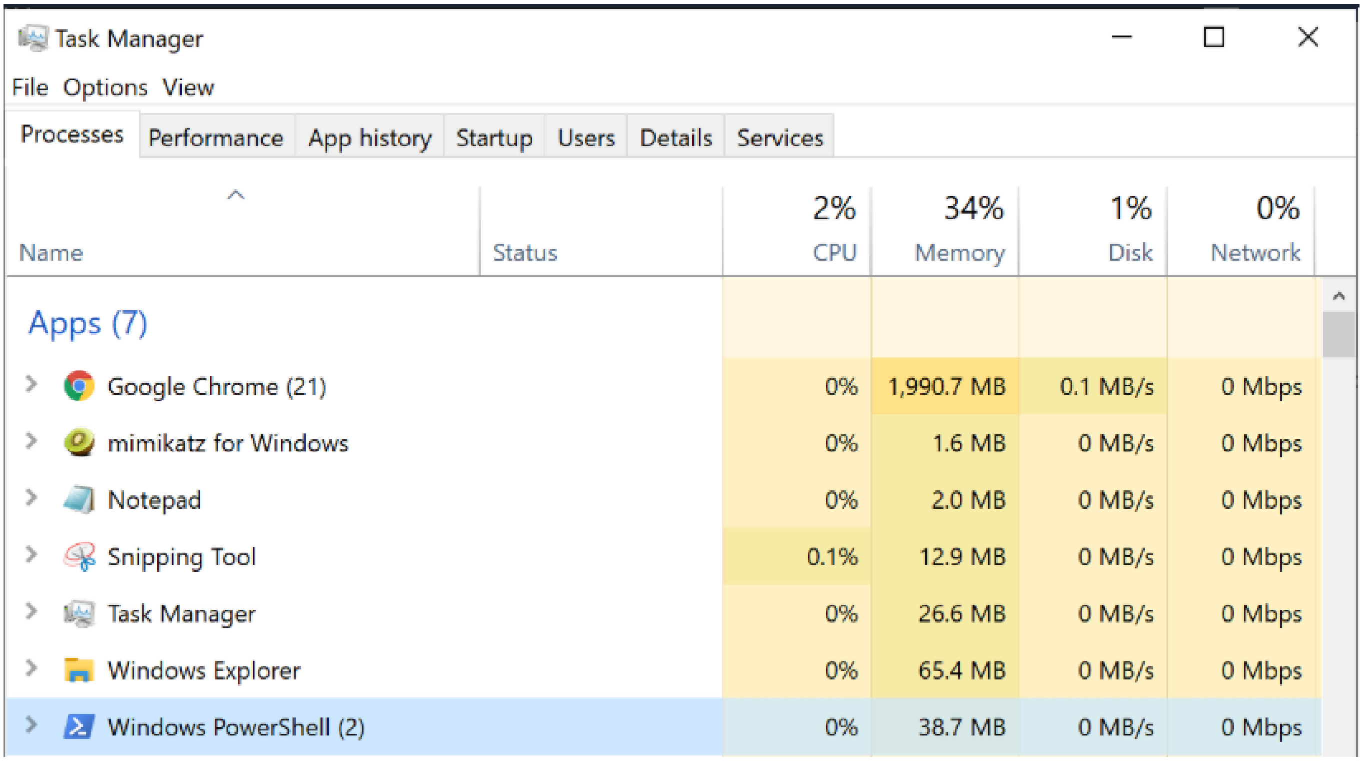
Sysinternals Tools

La suite **SysInternals Tools** es un conjunto de aplicaciones portátiles de Windows que permiten administrar sistemas Windows (generalmente sin necesidad de instalación). Las herramientas pueden descargarse del sitio web de Microsoft o cargarse directamente desde un recurso compartido de archivos con acceso a internet, escribiendo \live.sysinternals.com\tools en una ventana del Explorador de Windows.

Algunas de estas herramientas son:

Task Manager (Administrador de Tareas)

Proporciona información sobre los procesos en ejecución, el rendimiento del sistema, los servicios en ejecución, los programas de inicio, los usuarios conectados, sus procesos y los servicios.



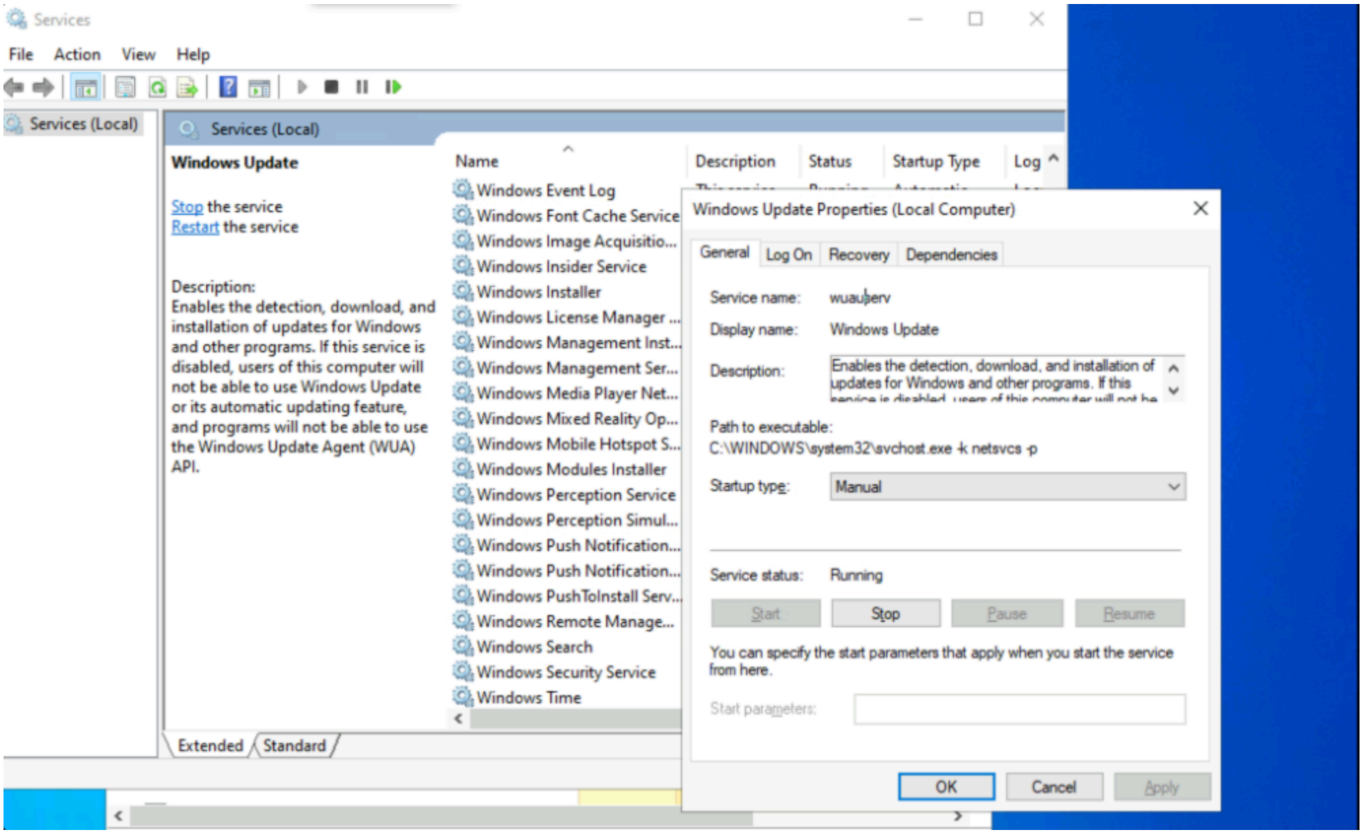
Name	Status	2% CPU	34% Memory	1% Disk	0% Network
Apps (7)					
Google Chrome (21)		0%	1,990.7 MB	0.1 MB/s	0 Mbps
mimikatz for Windows		0%	1.6 MB	0 MB/s	0 Mbps
Notepad		0%	2.0 MB	0 MB/s	0 Mbps
Snipping Tool		0.1%	12.9 MB	0 MB/s	0 Mbps
Task Manager		0%	26.6 MB	0 MB/s	0 Mbps
Windows Explorer		0%	65.4 MB	0 MB/s	0 Mbps
Windows PowerShell (2)		0%	38.7 MB	0 MB/s	0 Mbps

Service Permissions

Los administradores de sistemas suelen ignorarlos como posibles vectores de amenaza que los servicios pueden utilizarse para cargar DLL maliciosas, ejecutar aplicaciones sin acceso a una cuenta de administrador, escalar privilegios e incluso mantener la persistencia. Estos vectores de amenaza en los servicios de Windows suelen surgir debido a **configuraciones incorrectas** de permisos de servicio implementadas por software de terceros y errores que los administradores cometen fácilmente durante los procesos de instalación.

El primer paso para comprender la importancia de los permisos de servicio es simplemente comprender su existencia y tenerlos en cuenta. En sistemas operativos de servidor, los servicios de red críticos como DHCP y los Servicios de Dominio de Active Directory suelen instalarse utilizando la cuenta asignada al administrador que realiza la instalación. Parte del proceso de instalación incluye la asignación de un servicio específico para su ejecución con las credenciales y privilegios de un usuario designado, que, **por defecto**, se configura dentro del contexto del usuario conectado.

Examining Services using services.msc



Windows Update

Stop the service
Restart the service

Description:
Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.

Name
Windows Event Log
Windows Font Cache Service
Windows Image Acquisitio...
Windows Insider Service
Windows Installer
Windows License Manager ...
Windows Management Inst...
Windows Management Ser...
Windows Media Player Net...
Windows Mixed Reality Op...
Windows Mobile Hotspot S...
Windows Modules Installer
Windows Perception Service
Windows Perception Simul...
Windows Push Notification...
Windows Push Notification...
Windows PushToInstall Serv...
Windows Remote Manage...
Windows Search
Windows Security Service
Windows Time

Windows Update Properties (Local Computer)

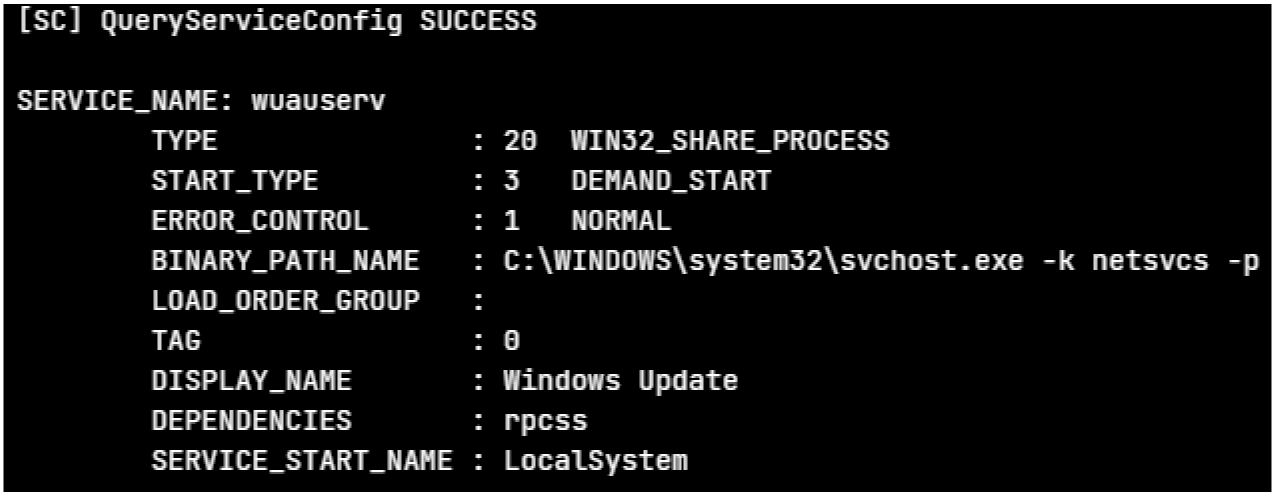
Service name: wuauserv
Display name: Windows Update
Description: Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be
Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs -p
Startup type: Manual
Service status: Running
You can specify the start parameters that apply when you start the service from here.
Start parameters:

Si los permisos NTFS del directorio de destino están configurados con **permisos débiles**, un atacante podría reemplazar el ejecutable original por uno creado con fines maliciosos.

La mayoría de los servicios se ejecutan con privilegios de sistema local de forma predeterminada, que es el nivel máximo de acceso permitido en un sistema operativo Windows. **No todas las aplicaciones necesitan permisos de cuenta de sistema local**, por lo que conviene investigar caso por caso al considerar la instalación de nuevas aplicaciones en un entorno Windows. Es recomendable identificar aplicaciones que puedan ejecutarse con el mínimo de privilegios posible para cumplir con el principio de **mínimo privilegio**.

Examining services using sc

```
sc qc wuauserv
```

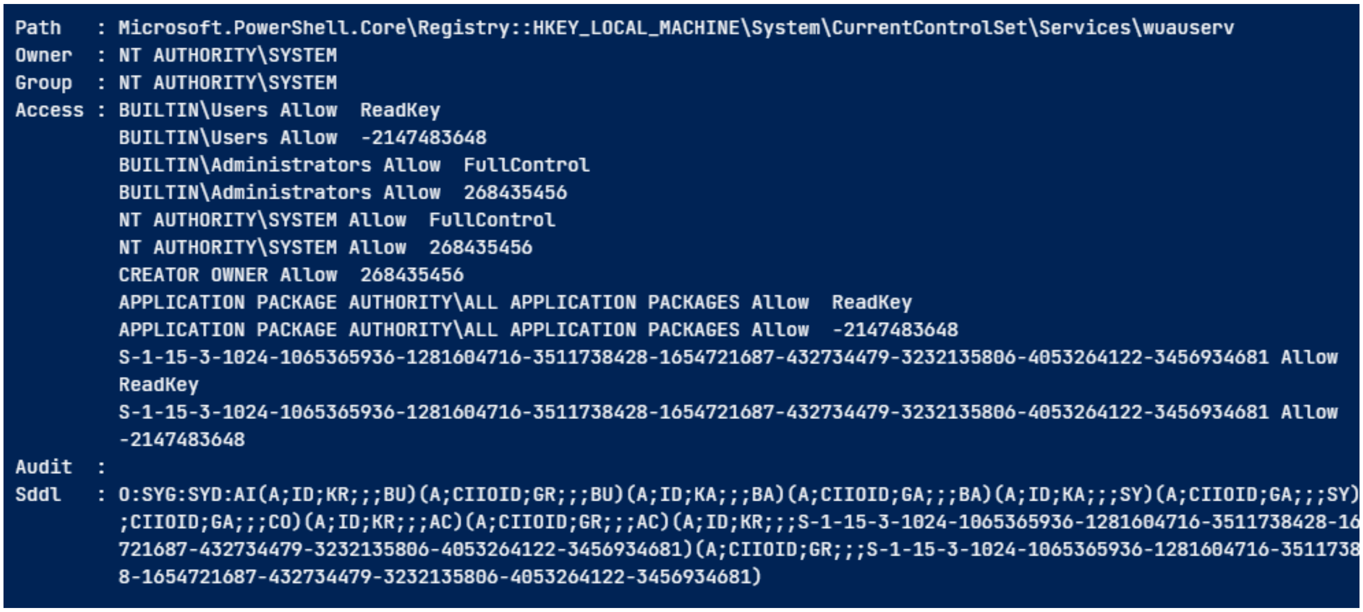


```
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: wuauserv
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\WINDOWS\system32\svchost.exe -k netsvcs -p
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Windows Update
        DEPENDENCIES       : rpcss
        SERVICE_START_NAME : LocalSystem
```

Examine service permissions using PowerShell

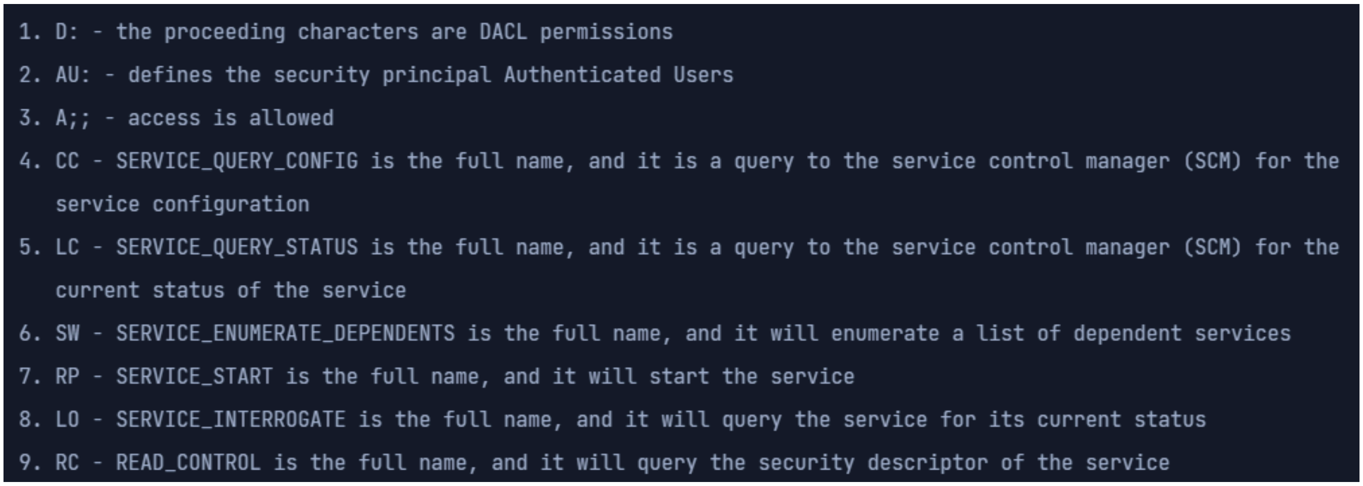
Usando el **Get-Acl** de PowerShell, podemos examinar los permisos del servicio apuntando a la ruta de un servicio específico en el registro.

```
Get-ACL -Path HKLM:\System\CurrentControlSet\Services\wuauserv | Format-List
```



```
Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wuauserv
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Users Allow  ReadKey
         BUILTIN\Users Allow  -2147483648
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow
         ReadKey
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow
         -2147483648
Audit  :
Sddl   : O:SYG:SYD:AI(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)
         ;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-16
         721687-432734479-3232135806-4053264122-3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738
         8-1654721687-432734479-3232135806-4053264122-3456934681)
```

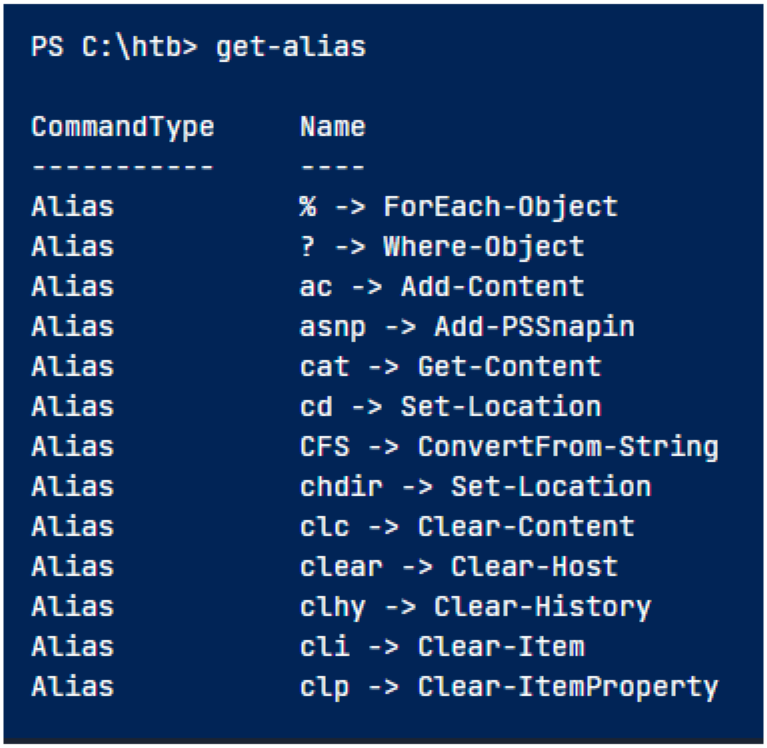
El output de los servicios según **Security Descriptor Definition Language** (Sddl) te puede traducir con:



```
1. D: - the proceeding characters are DACL permissions
2. AU: - defines the security principal Authenticated Users
3. A;; - access is allowed
4. CC - SERVICE_QUERY_CONFIG is the full name, and it is a query to the service control manager (SCM) for the
   service configuration
5. LC - SERVICE_QUERY_STATUS is the full name, and it is a query to the service control manager (SCM) for the
   current status of the service
6. SW - SERVICE_ENUMERATE_DEPENDENTS is the full name, and it will enumerate a list of dependent services
7. RP - SERVICE_START is the full name, and it will start the service
8. LO - SERVICE_INTERROGATE is the full name, and it will query the service for its current status
9. RC - READ_CONTROL is the full name, and it will query the security descriptor of the service
```

Interacting with the Windows Operating System

PowerShell and CMD commands

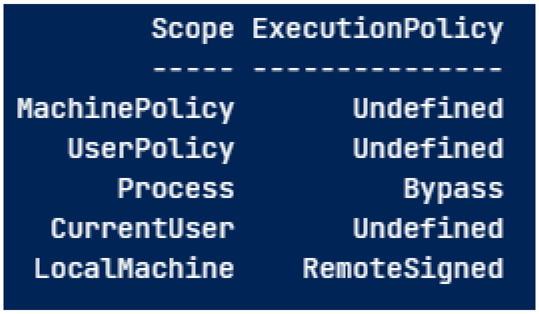


```
PS C:\htb> get-alias

CommandType     Name
-----------     ----
Alias           % -> ForEach-Object
Alias           ? -> Where-Object
Alias           ac -> Add-Content
Alias           asnp -> Add-PSSnapin
Alias           cat -> Get-Content
Alias           cd -> Set-Location
Alias           CFS -> ConvertFrom-String
Alias           chdir -> Set-Location
Alias           clc -> Clear-Content
Alias           clear -> Clear-Host
Alias           clhy -> Clear-History
Alias           cli -> Clear-Item
Alias           clp -> Clear-ItemProperty
```

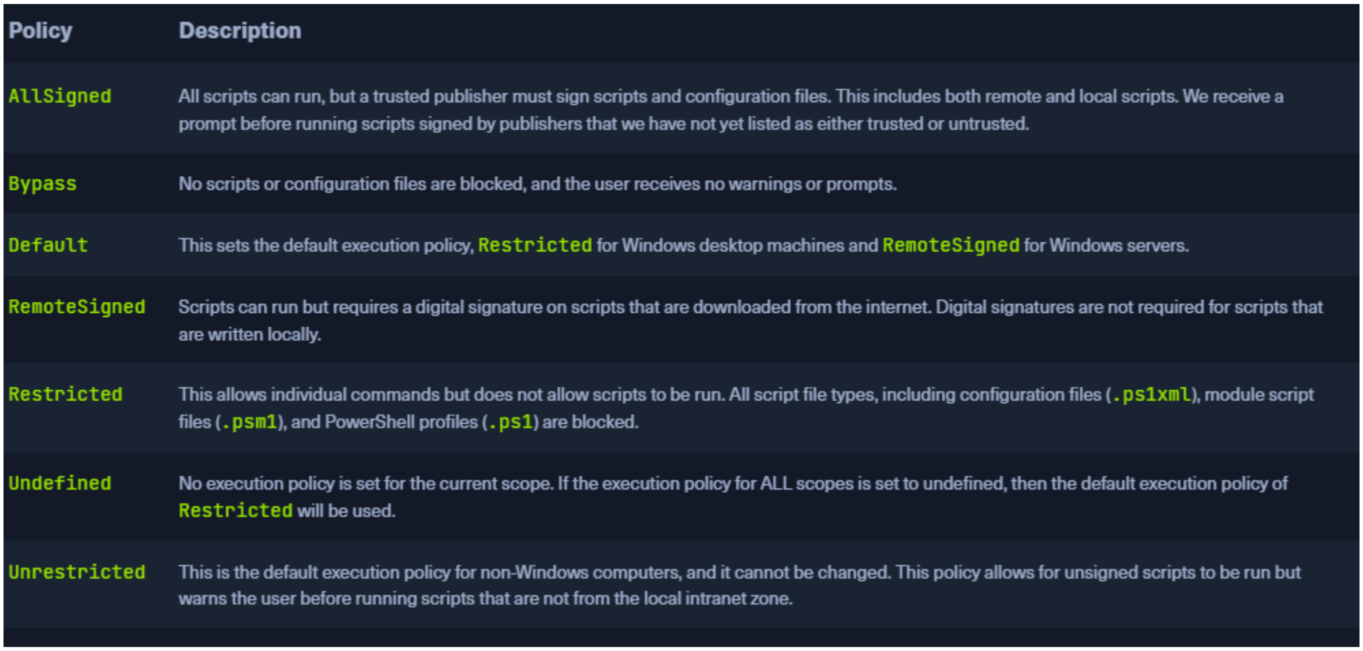
Execution Policy

Para saber la política de ejecución de los alcances (Scope) utilizamos:

```
Get-ExecutionPolicy -List
```

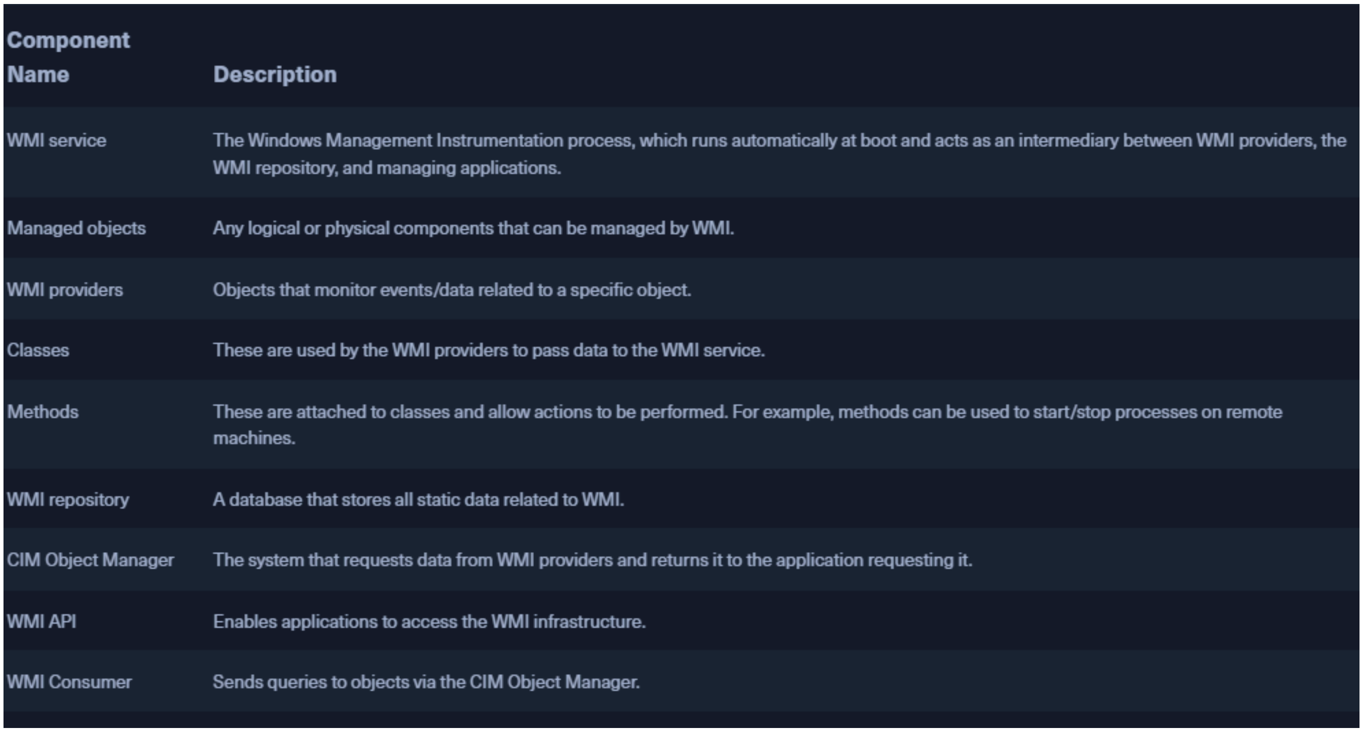


```
        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process          Bypass
  CurrentUser       Undefined
 LocalMachine    RemoteSigned
```



Policy	Description
`AllSigned`	All scripts can run, but a trusted publisher must sign scripts and configuration files. This includes both remote and local scripts. We receive a prompt before running scripts signed by publishers that we have not yet listed as either trusted or untrusted.
`Bypass`	No scripts or configuration files are blocked, and the user receives no warnings or prompts.
`Default`	This sets the default execution policy, `Restricted` for Windows desktop machines and `RemoteSigned` for Windows servers.
`RemoteSigned`	Scripts can run but requires a digital signature on scripts that are downloaded from the internet. Digital signatures are not required for scripts that are written locally.
`Restricted`	This allows individual commands but does not allow scripts to be run. All script file types, including configuration files (`.ps1xml`), module script files (`.psm1`), and PowerShell profiles (`.ps1`) are blocked.
`Undefined`	No execution policy is set for the current scope. If the execution policy for ALL scopes is set to undefined, then the default execution policy of `Restricted` will be used.
`Unrestricted`	This is the default execution policy for non-Windows computers, and it cannot be changed. This policy allows for unsigned scripts to be run but warns the user before running scripts that are not from the local intranet zone.

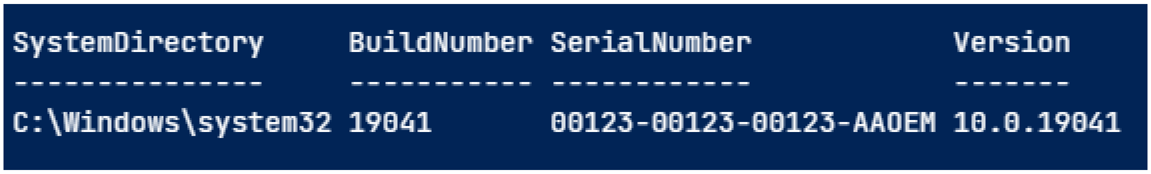
Windows Management Instrumentation (WMI)



Component Name	Description
WMI service	The Windows Management Instrumentation process, which runs automatically at boot and acts as an intermediary between WMI providers, the WMI repository, and managing applications.
Managed objects	Any logical or physical components that can be managed by WMI.
WMI providers	Objects that monitor events/data related to a specific object.
Classes	These are used by the WMI providers to pass data to the WMI service.
Methods	These are attached to classes and allow actions to be performed. For example, methods can be used to start/stop processes on remote machines.
WMI repository	A database that stores all static data related to WMI.
CIM Object Manager	The system that requests data from WMI providers and returns it to the application requesting it.
WMI API	Enables applications to access the WMI infrastructure.
WMI Consumer	Sends queries to objects via the CIM Object Manager.

Si queremos obtener el número de serie de un dispositivo nos basta con:

```
Get-WmiObject -Class Win32_OperatingSystem | select
SystemDirectory,BuildNumber,SerialNumber,Version | ft
```



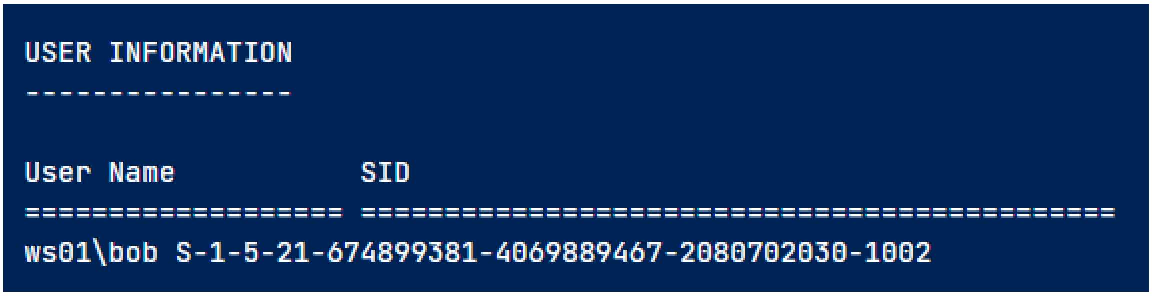
```
SystemDirectory     BuildNumber SerialNumber            Version
---------------     ----------- ------------            -------
C:\Windows\system32 19041       00123-00123-00123-AAOEM 10.0.19041
```

Windows Security

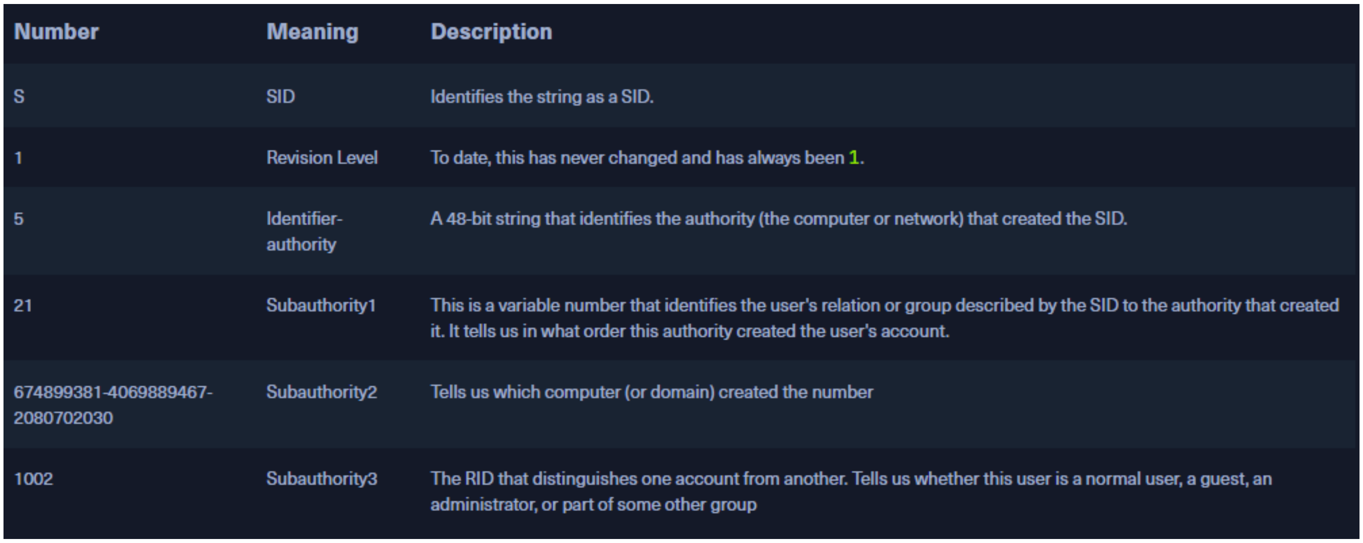
Security Identifier (SID)

Un SID consta de la Autoridad de Identificación y el ID Relativo (RID). En un entorno de dominio de Active Directory (AD), el SID también incluye el SID del dominio.

```
PS C:\htb> whoami /user
```



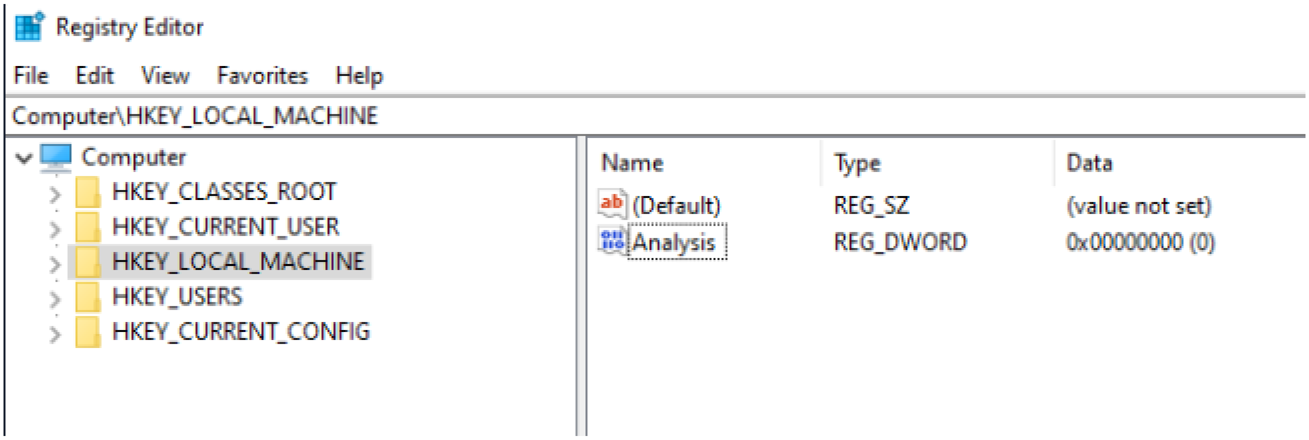
```
USER INFORMATION
----------------

User Name           SID
=================== =============================================
ws01\bob S-1-5-21-674899381-4069889467-2080702030-1002
```



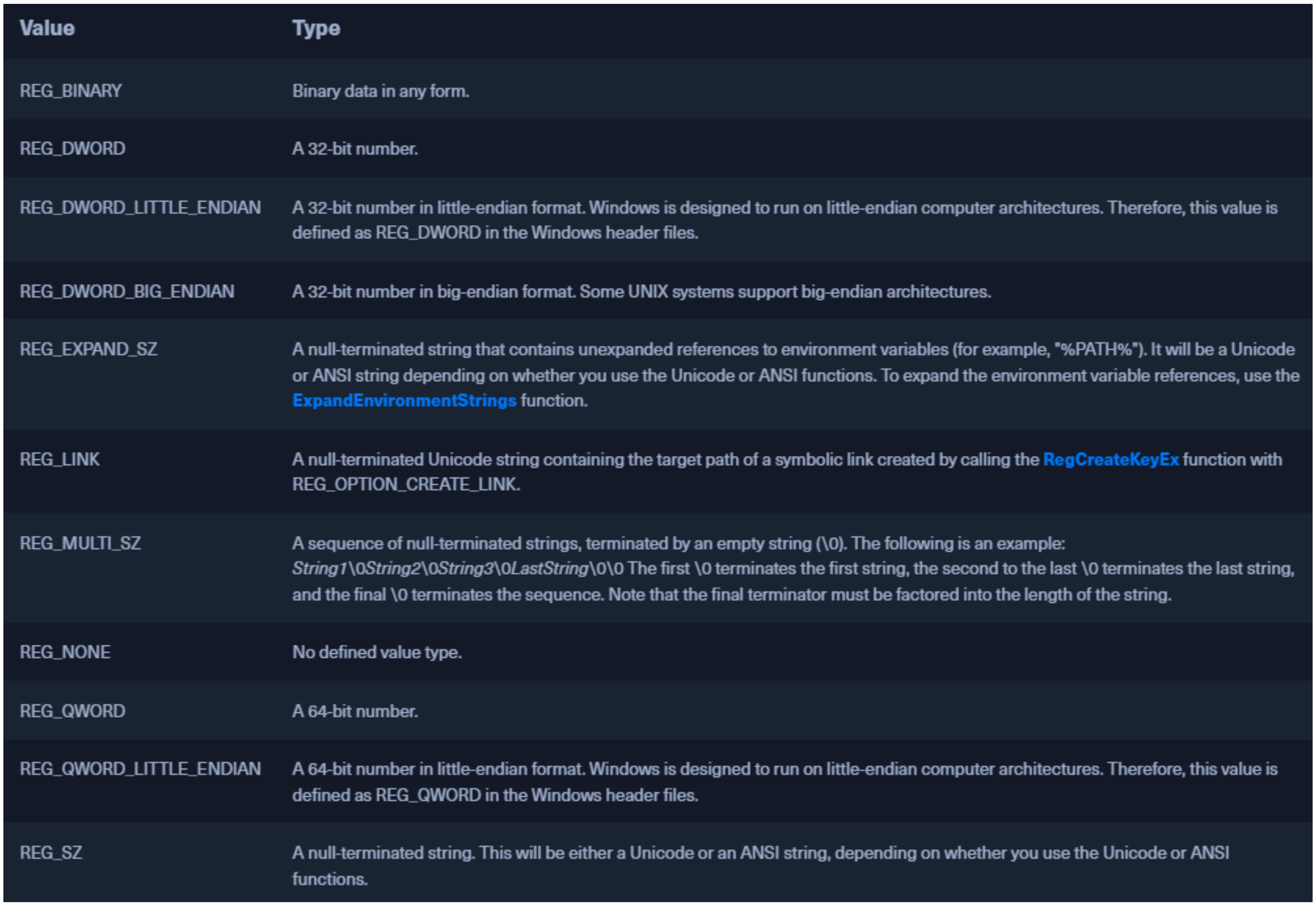
Number	Meaning	Description
S	SID	Identifies the string as a SID.
1	Revision Level	To date, this has never changed and has always been 1.
5	Identifier-authority	A 48-bit string that identifies the authority (the computer or network) that created the SID.
21	Subauthority1	This is a variable number that identifies the user's relation or group described by the SID to the authority that created it. It tells us in what order this authority created the user's account.
674899381-4069889467-2080702030	Subauthority2	Tells us which computer (or domain) created the number
1002	Subauthority3	The RID that distinguishes one account from another. Tells us whether this user is a normal user, a guest, an administrator, or part of some other group

Registry

El Registro es una base de datos jerárquica de Windows, crucial para el sistema operativo. **Almacena la configuración de bajo nivel** del sistema operativo Windows y de las aplicaciones que lo utilizan. **Se divide en datos específicos del equipo y del usuario**. Podemos abrir el Editor del Registro escribiendo **regedit** desde la línea de comandos o la barra de búsqueda de Windows.



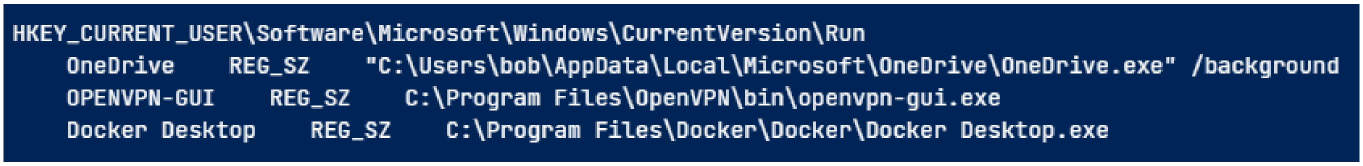
Name	Type	Data
(Default)	REG_SZ	(value not set)
Analysis	REG_DWORD	0x00000000 (0)



Value	Type
REG_BINARY	Binary data in any form.
REG_DWORD	A 32-bit number.
REG_DWORD_LITTLE_ENDIAN	A 32-bit number in little-endian format. Windows is designed to run on little-endian computer architectures. Therefore, this value is defined as REG_DWORD in the Windows header files.
REG_DWORD_BIG_ENDIAN	A 32-bit number in big-endian format. Some UNIX systems support big-endian architectures.
REG_EXPAND_SZ	A null-terminated string that contains unexpanded references to environment variables (for example, "%PATH%"). It will be a Unicode or ANSI string depending on whether you use the Unicode or ANSI functions. To expand the environment variable references, use the **ExpandEnvironmentStrings** function.
REG_LINK	A null-terminated Unicode string containing the target path of a symbolic link created by calling the **RegCreateKeyEx** function with REG_OPTION_CREATE_LINK.
REG_MULTI_SZ	A sequence of null-terminated strings, terminated by an empty string (\0). The following is an example: *String1*\0*String2*\0*String3*\0*LastString*\0\0 The first \0 terminates the first string, the second to the last \0 terminates the last string, and the final \0 terminates the sequence. Note that the final terminator must be factored into the length of the string.
REG_NONE	No defined value type.
REG_QWORD	A 64-bit number.
REG_QWORD_LITTLE_ENDIAN	A 64-bit number in little-endian format. Windows is designed to run on little-endian computer architectures. Therefore, this value is defined as REG_QWORD in the Windows header files.
REG_SZ	A null-terminated string. This will be either a Unicode or an ANSI string, depending on whether you use the Unicode or ANSI functions.

Para saber que aplicación de seguridad de terceros está deshabilitada al inicio para el usuario actual:

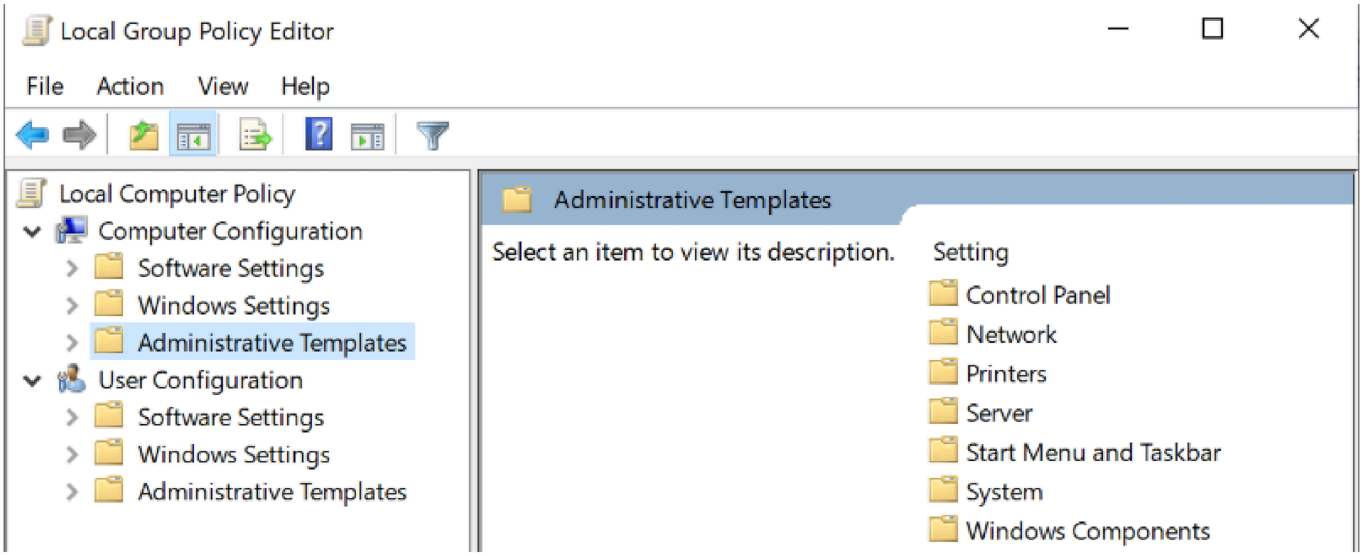
```
reg query
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```



```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    OneDrive    REG_SZ    "C:\Users\bob\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
    OPENVPN-GUI    REG_SZ    C:\Program Files\OpenVPN\bin\openvpn-gui.exe
    Docker Desktop    REG_SZ    C:\Program Files\Docker\Docker\Docker Desktop.exe
```

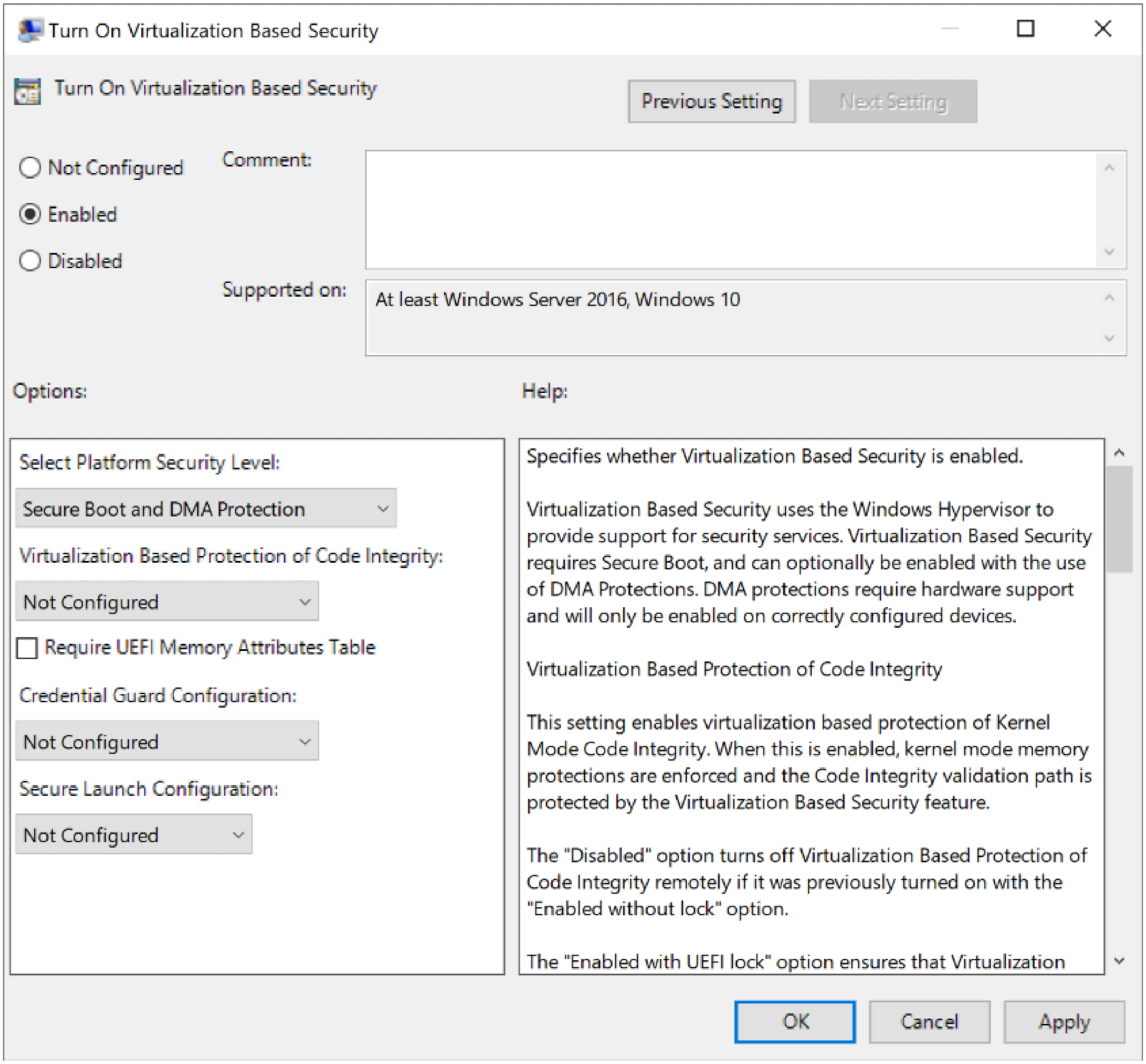
Local Group Policy

La directiva de grupo permite a los administradores **establecer, configurar y ajustar diversas opciones**. En un entorno de dominio, las directivas de grupo se implementan desde un controlador de dominio en todas las máquinas unidas al dominio a las que están vinculados objetos de directiva de grupo (GPO). Estas configuraciones también se pueden definir en máquinas individuales mediante la directiva de grupo local.



Select an item to view its description.

Por ejemplo, podemos abrir la Directiva de equipo local para habilitar Credential Guard activando la opción "Activar seguridad basada en virtualización". Credential Guard es una función de Windows 10 que protege contra ataques de robo de credenciales al aislar el proceso LSA del sistema operativo.



Turn On Virtualization Based Security

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10

Options:

Select Platform Security Level: Secure Boot and DMA Protection

Virtualization Based Protection of Code Integrity: Not Configured

□ Require UEFI Memory Attributes Table

Credential Guard Configuration: Not Configured

Secure Launch Configuration: Not Configured

Help:

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.

Virtualization Based Protection of Code Integrity

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

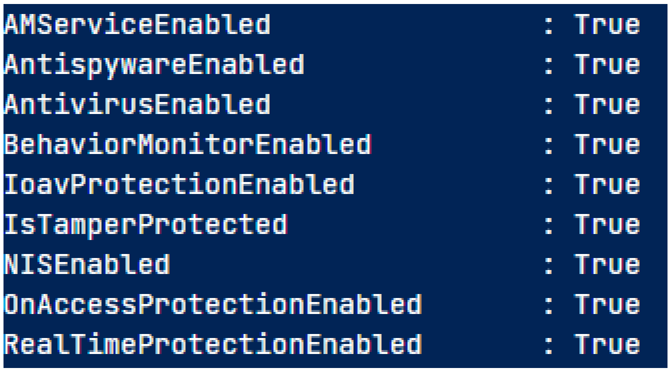
The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

The "Enabled with UEFI lock" option ensures that Virtualization

Windows Defender Antivirus

Para ver si tenemos los servicios de seguridad activos:

```
Get-MpComputerStatus | findstr "True"
```



```
AMServiceEnabled                 : True
AntispywareEnabled               : True
AntivirusEnabled                 : True
BehaviorMonitorEnabled           : True
IoavProtectionEnabled            : True
IsTamperProtected                : True
NISEnabled                       : True
OnAccessProtectionEnabled        : True
RealTimeProtectionEnabled        : True
```

Skills Assessment - Windows Fundamentals

Para listar el SID de un usuario:

```
wmic useraccount get name, ssid
```

Para listar el SID de un grupo:

```
wmic group get name, ssid
```

Para ver el nombre de los servicios que están corriendo en el dispositivo:

```
get-service
```