Administración de software de base (Implantación de sistemas operativos)

Administración de usuarios y grupos locales

Los sistemas operativos actuales se pueden utilizar por uno o varios usuarios, en algunos sistemas pueden hacerlo simultáneamente y en otros no. Los usuarios se pueden crear localmente o en red, la gestión de usuarios locales sólo afecta al equipo desde el que se crean, modifican, eliminan, etc.

Los usuarios locales sólo sirven para iniciar sesión o acceder a recursos en el propio equipo, en cambio los usuarios en red pueden iniciar sesión en cualquier equipo de la red.

En la mayoría de los sistemas operativos, las personas que los utilizan necesitan autentificarse mediante una cuenta de usuario y, además, tener autorización para utilizar recursos como, por ejemplo, un archivo, una carpeta, un dispositivo, etc. Cuando hablamos de recursos, nos referimos a un elemento del sistema operativo que se puede controlar.

Algunas de las gestiones sobre usuarios y grupos que veremos hacen referencia a configuraciones propias de sistemas operativos en red (Windows Server) con instalaciones de un Directorio Activo (Active Directory).

Usuarios y grupos predeterminados

Usuarios

Las personas que quieren utilizar un sistema operativo necesitan disponer de un nombre de usuario y una contraseña.

Los usuarios deberían ser únicos e individuales aunque a veces no es así, esto conlleva un importante riesgo de seguridad porque no se identifica correctamente a los usuarios dentro del sistema.

Para crear un usuario es necesario tener permisos especiales, no todos los usuarios pueden crear otros usuarios.

A la hora de crear un usuario hay que seguir algunas normas que facilitarán recordar los nombres y llevar un correcto control.

Las operaciones con usuarios son tareas de administración que sólo pueden ser realizadas por usuarios administradores.

Ejercicios

Crear una función que indica si existe o no un usuario

- https://www.jesusninoc.com/01/13/ejercicios-de-powershell-crear-una-funcion-que-indica-si-existe-o-no-un-usuario/

Verificar que existe un usuario mediante el cmdlet Get-LocalUser

- https://www.jesusninoc.com/01/13/ejercicios-de-powershell-verificar-que-existe-un-usuario-mediante-el-cmdlet-get-localuser/

Crear una función que dice si un usuario existe o no (mostrando si existe o no)

- https://www.jesusninoc.com/01/09/ejercicios-de-powershel

l-crear-una-funcion-que-dice-si-un-usuario-existe-o-no-mostrando-si-existe-o-no-con-read-host/

Crear una función que dice si un usuario existe o no (mostrando si existe o no, con Read-Host y aceptar minúsculas)

- https://www.jesusninoc.com/01/10/ejercicios-de-powershell-crear-una-funcion-que-dice-si-un-usuario-existe-o-no-mostrando-si-existe-o-no-con-read-host-y-aceptar-minusculas/

Crear una función que indica el SID de los usuarios

- https://www.jesusninoc.com/01/06/ejercicios-de-powershell-crear-una-funcion-que-indica-el-sid-de-los-usuarios/

Iniciar un programa siendo otro usuario

- https://www.jesusninoc.com/01/11/ejercicios-de-powershell-iniciar-un-programa-siendo-otro-usuario/

Crear una función que indique el nombre del usuario leyendo un SID

- https://www.jesusninoc.com/01/13/ejercicios-de-powershell-crear-una-funcion-que-indique-el-nombre-del-usuario-leyendo-un-sid/

Crear una función que lea SID de un fichero e indique el nombre del usuario

- https://www.jesusninoc.com/01/13/ejercicios-de-powershell-crear-una-funcion-que-lea-sid-de-un-fichero-e-indique-el-nombre-del-usuario/

Crear una función que lea los nombres de usuarios en un fichero e indique el SID de cada uno de ellos

- https://www.jesusninoc.com/01/13/ejercicios-de-powershell-crear-una-funcion-que-lea-los-nombres-de-usuarios-en-un-fichero-e-indique-el-sid-de-cada-uno-de-ellos/

Más información

¿Qué es el número de sesiones de usuario?

- https://www.jesusninoc.com/01/12/introduccion-a-los-sistemas-operativos/#El_numero_de_sesiones

Usuarios en PowerShell

- https://www.jesusninoc.com/07/08/8-gestion-de-usuarios-en-powershell/

Grupos

Un grupo es un conjunto de usuarios que simplifica la administración y la asignación de permisos, concediendo permisos sobre recursos a todo un grupo de usuarios a la vez, en lugar de concederlos a cuentas de usuarios individuales. Los usuarios pueden pertenecer o no pertenecer a uno o varios grupos distintos.

En Windows los usuarios se pueden asociar en grupos y de esta forma se pueden asignar permisos para el acceso a determinados recursos. Los grupos locales predeterminados se crean automáticamente al instalar el sistema operativo.

Las operaciones con usuarios son tareas de administración que sólo pueden ser realizadas por usuarios administradores.

Seguridad de cuentas de usuario

Las principales características que están relacionadas con la gestión de la seguridad de usuario y grupos son (algunas características hacen referencia a sistemas operativos clientes y otras a servidores, aunque la mayoría a ambos):

Cuenta de usuario

La cuenta de usuario consiste en un nombre de usuario y una contraseña (password), en algunos sistemas operativos estos dos elementos forman un conjunto de credenciales y sirven para identificar a una persona.

Utilizar contraseñas es un método para autentificarse, pero no es el único, hay otros métodos como, por ejemplo, el uso de tarjetas inteligentes que tiene la identidad grabada.

Los usuarios tienen distintos privilegios y restricciones, el usuario que más privilegios tiene es el administrador.

Más información

- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-enviar-credenciales-entre-un-cliente-y-un-servidor-por-udp-y-ejecutar-una-aplicacion-en-el-servidor-con-dichos-credenciales/

Listas de control de acceso

Para utilizar recursos se requiere tener autorización, cada recurso tiene una lista donde aparecen los usuarios que pueden usar dicho recurso, estas listas se conocen como ACL (Access Control List, o Lista de control de acceso).

El funcionamiento es el siguiente: cuando un usuario intenta acceder a un recurso, éste comprueba en la lista de control de acceso si el usuario tiene permiso o no para utilizarlo. La lista de control de acceso se compone de identificadores de seguridad (SID, Security IDentifier) y permisos.

Los identificadores de seguridad son unos valores únicos de

longitud variable que se utilizan para identificar a usuarios y grupos.

Control de cuentas de usuario

Esta característica de seguridad informa a los usuarios mediante mensajes sobre los cambios que se realizan en el equipo.

Las notificaciones son distintas dependiendo del tipo de usuario que haya iniciado la sesión, en el caso de ser administrador, se solicita aceptar o denegar; si es un usuario normal, se solicitan las credenciales del administrador (usuario y contraseña).

Ejecutar como

Iniciar sesión con credenciales de administrador puede suponer un riesgo para la seguridad del sistema operativo y de la red (en el caso de que el ordenador forme parte). El riesgo se debe a que los usuarios administradores pueden realizar cualquier tipo de cambio en el sistema y puede darse el caso de que el administrador ejecute un programa dañino para el sistema como, por ejemplo, un virus, por este motivo, es recomendable iniciar sesión con usuarios no administradores.

Perfil de usuario

Los perfiles de usuario definen entornos de escritorio personalizados, en ellos se incluye la configuración de cada usuario como, por ejemplo, la configuración de la pantalla, las conexiones de red y de impresoras, otras configuraciones especificadas, etc. El usuario o el administrador del sistema pueden definir las características del entorno del escritorio. La personalización del entorno de escritorio efectuada por un usuario no afecta a la configuración del resto de los usuarios.

Cuando los usuarios inician de nuevo la sesión en sus estaciones de trabajo, reciben la configuración de escritorio que tenían al terminar la última sesión.

Directivas de Grupo

Las directivas permiten a los administradores configurar el sistema operativo, estas configuraciones se pueden hacer en **local o en red**, en este apartado veremos las dos configuraciones. Las configuraciones de Directivas de Grupo se realizan desde los servidores (Windows Server) y se aplican a los equipos clientes.

Seguridad de contraseñas

Las contraseñas deben satisfacer unos requisitos de complejidad, con los siguientes ejemplos tenemos algunos requisitos que deberían cumplir:

- La contraseña no aparece en un diccionario.
- La contraseña no tiene un hash que aparece en los buscadores.
- La contraseña tiene una longitud correcta.
- La contraseñas no aparece en los buscadores.

Ejercicio

Generar letras aleatorias

- https://www.jesusninoc.com/2017/10/11/generar-letras-aleatorias/

Más información

Contraseñas seguras

- https://www.jesusninoc.com/08/27/contrasenas-seguras-con-powershell-generar-contrasenas-seguras/
- https://www.jesusninoc.com/07/03/contrasenas-seguras-con-powershell-longitud-de-la-contrasena/
- https://www.jesusninoc.com/10/20/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-el-diccionario-de-la-rae/
- https://www.jesusninoc.com/07/07/contrasenas-seguras-con-powershell-convertir-en-hash-una-contrasena/
- https://www.jesusninoc.com/07/05/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-google/
- https://www.jesusninoc.com/07/06/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-un-diccionario/

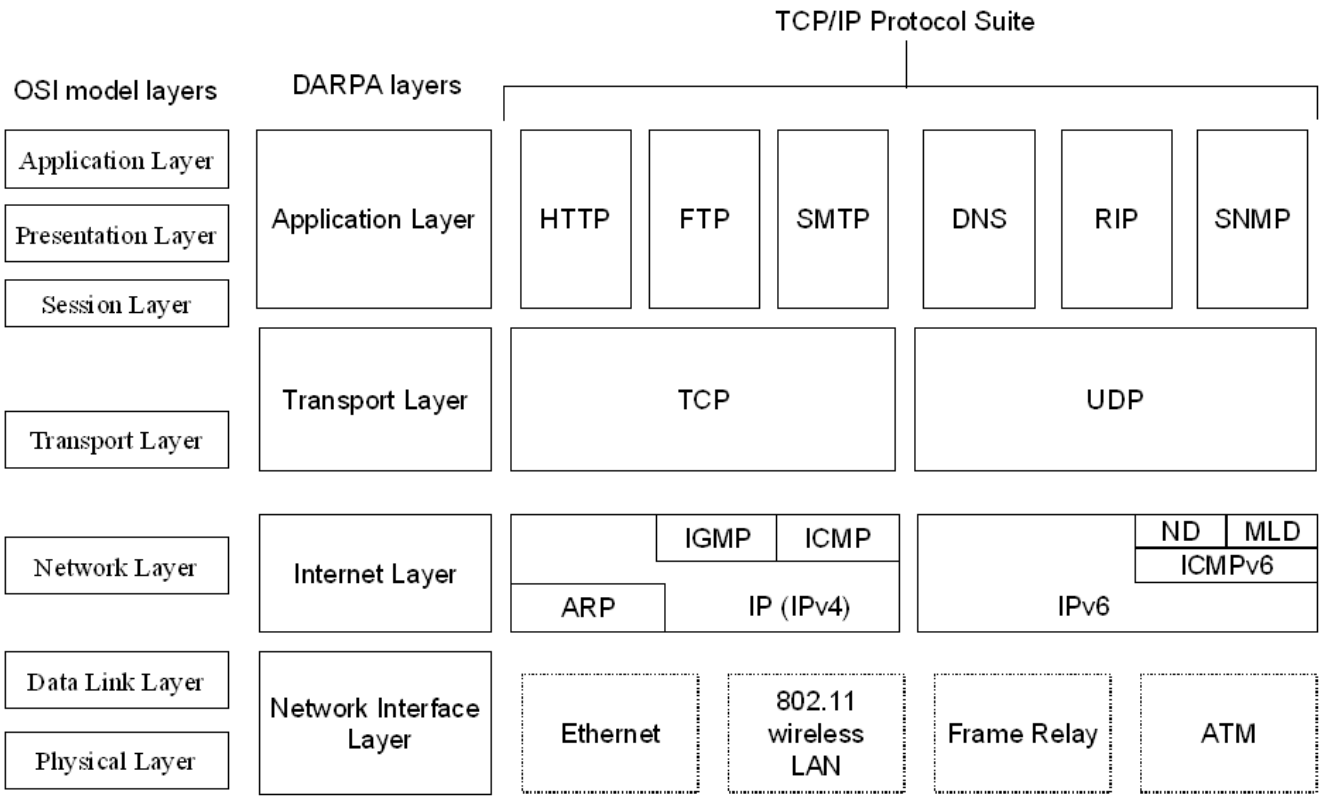
Hash en Windows (NT4)

- https://www.jesusninoc.com/01/27/creacion-de-hashes-de-contrasena-nt4/

Administración de perfiles locales de usuario

Los perfiles de usuario definen entornos de escritorio personalizados, en ellos se incluye la configuración de cada usuario como, por ejemplo, la configuración de la pantalla, las conexiones de red y de impresoras, otras configuraciones especificadas, etc. El usuario o el administrador del sistema pueden definir las características del entorno del escritorio. La personalización del entorno de escritorio efectuada por un usuario no afecta a la configuración del resto de los usuarios.

Configuración del protocolo TCP/IP en un cliente de red



Relación de las capas del modelo TCP/IP con PowerShell:

Capa física

La capa de red física especifica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe por ejemplo los estándares de hardware como IEEE 802.3 y la especificación del medio de red Ethernet.

Capa de Internet

La capa de Internet, también conocida como capa de red o capa IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

Capa de transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP). El protocolo TCP proporciona un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

Más información

- https://www.jesusninoc.com/07/09/9-gestion-de-la-red-en-powershell/

Ejercicios

Realizar una comunicación entre dos ordenadores por UDP desde PowerShell

- https://www.jesusninoc.com/01/30/enviar-un-mensaje-udp-entre-dos-equipos-desde-powershell/
- https://www.jesusninoc.com/01/30/realizar-una-comunicacion-entre-dos-ordenadores-por-udp-desde-powershell/
- https://www.jesusninoc.com/02/03/enviar-el-nombre-un-usuario-al-servidor-por-udp/
- https://www.jesusninoc.com/02/03/enviar-el-nombre-un-usuario-al-servidor-por-udp-y-que-el-servidor-abra-una-pagina-web-con-el-nombre-recibido/
- https://www.jesusninoc.com/02/03/enviar-un-mensaje-a-un-servidor-con-udp-y-que-el-servidor-responda-con-hola-cliente-independientemente-del-nombre-del-usuario/
- https://www.jesusninoc.com/02/03/enviar-un-nombre-usuario-a-un-servidor-con-udp-y-si-es-correcto-el-servidor-

responde-al-cliente-con-el-contenido-de-una-pagina-web-que-el-cliente-abre-con-google-chrome/

Realizar una comunicación entre dos ordenadores por UDP desde PowerShell

- https://www.jesusninoc.com/10/26/crear-una-comunicacion-entre-un-cliente-en-powershell-de-windows-y-un-servidor-en-bash-de-linux-utilizando-tcpip/

Relacionar las conexiones que están abiertas (TCP o UDP) con los procesos que se están ejecutando en el sistema con PowerShell

- https://www.jesusninoc.com/02/04/ejercicios-de-powershell-sacar-los-nombre-de-los-procesos-de-cada-conexion-de-red-tcp/
- https://www.jesusninoc.com/02/05/ejercicios-de-powershell-sacar-el-nombre-del-proceso-que-abre-cada-conexion-de-red-tcp-junto-con-la-direccion-ip-remota/
- https://www.jesusninoc.com/02/05/sacar-el-nombre-del-proceso-que-abre-cada-conexion-de-red-udp-junto-con-la-direccion-ip-local/

Comprobar si los puertos (TCP o UDP) están abiertos en PowerShell

- https://www.jesusninoc.com/02/05/ejercicios-de-powershell-ver-los-puertos-locales-que-estan-abiertos-en-nuestro-equipo-tcp-y-udp/
- https://www.jesusninoc.com/02/05/ejercicios-de-powershell-comprobar-los-puertos-tcp-abiertos-de-un-rango-a-otro-mediante-un-try-y-un-catch-e-indicar-si-esta-abierto-o-no-el-puerto-si-hace-lo-que-queremos/
- https://www.jesusninoc.com/02/05/ejercicios-de-powershell-listar-las-direcciones-ip-remotas-que-utilizan-el-protocolo-tcp-e-indicar-la-resolucion-dns/

Comunicación entre cliente y servidor

- https://www.jesusninoc.com/2015/02/25/creating-reverse-s

hell/
- https://www.jesusninoc.com/2015/02/26/creating-shell/
- https://www.jesusninoc.com/2017/10/18/crear-una-comunicacion-entre-un-cliente-en-bash-de-linux-y-un-servidor-en-powershell-de-windows-utilizando-tcpip/
- https://www.jesusninoc.com/2017/10/26/crear-una-comunicacion-entre-un-cliente-en-powershell-de-windows-y-un-servidor-en-bash-de-linux-utilizando-tcpip/
- https://www.jesusninoc.com/2016/04/30/simular-el-funcionamiento-de-un-servidor-web-utilizando-netcat-en-linux/
- https://www.jesusninoc.com/2009/06/06/ejecutar-nc-exe-cmd-exe-remotamente/

Servidor desde PowerShell

- https://www.jesusninoc.com/2017/05/06/crear-un-servidor-web-al-que-se-pueda-acceder-desde-cualquier-parte-de-la-red-privada-con-powershell/

Utilizando la comunicación remota entre cliente y servidor simular una conexión a una shell y una reverse shell

- https://www.jesusninoc.com/01/27/ejecutar-un-cmdlet-remotamente-en-un-equipo-utilizando-sockets-udp/
- https://www.jesusninoc.com/2015/02/25/creating-reverse-shell/
- https://www.jesusninoc.com/2015/02/26/creating-shell/

Ejecutar un comando remotamente utilizando un servidor web creado en PowerShell

- https://www.jesusninoc.com/12/18/ejercicios-de-powershell-ejecutar-un-comando-remotamente-utilizando-un-servidor-web-creado-en-powershell/

Capa de aplicación

La capa de aplicación define las aplicaciones de red y los

servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos.

Existen varios protocolos de capa de aplicación. En la lista siguiente se incluyen ejemplos de protocolos de capa de aplicación, algunos ejemplos son:

- Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.
- Servicios de nombres, como NIS o el sistema de nombre de dominio (DNS).
- Servicios de directorio (LDAP).

Configuración de la resolución de nombres

El sistema de nombre de dominio (DNS) es el servicio de nombres que proporciona Internet para las redes TCP/IP. DNS proporciona nombres de host al servicio de direcciones IP. También actúa como base de datos para la administración del correo.

El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

Ficheros de configuración de red

Los sistemas operativos se pueden conectar a la red de diversas formas, lo primero que hay que tener en cuenta es el dispositivo que permite la conexión a la red y lo segundo cómo se configura dicho dispositivo.

Se pueden utilizar varios dispositivos para realizar una conexión, por ejemplo un modem (puede ser USB o no) con un cable RJ-11, una tarjeta de red con un cable RJ-45, una tarjeta inalámbrica, etc.

Los parámetros de configuración básicos para una red son la dirección IP, la máscara de red, la puerta de enlace (Gateway) y los DNS. Veamos brevemente que es cada parámetro:

- La dirección IP (Internet Protocol, Protocolo de Internet) es un código que identifica a un interfaz como único, el interfaz es un dispositivo como una tarjeta de red, un punto de acceso, etc. Hay distintas versiones de direcciones IP:
    - La IPv4 está formada por un número binario de 32 bits, que normalmente se representa como 4 números en base decimal del 0 al 255, separados por puntos. Ejemplo: Dirección localhost en IPv4: 127.0.0.1
    - La otra versión es la IPv6 que son un número de 128 bits, representado en hexadecimal con 32 dígitos, separados por dos puntos en grupos de 4 dígitos. Ejemplo: Direccion localhost en IPv6: 0:0:0:0:0:0:0:1
- La máscara sirve para saber si se deben enviar los datos dentro o fuera de las redes. Por ejemplo, si el sistema operativo tiene la IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras ips, para fuera (internet, otra red local mayor…).
- Un Gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. El valor de la puerta de enlace es

otro de los valores que se deben indicar a la hora de configurar la conexión de red.
- Los DNS son dirección IP que sirven para resolver los nombres de dominio FQDN (Fully Qualified Domain Names) y traducirlos a direcciones IPv4.

Los parámetros que acabamos de ver se pueden asignar de las siguientes formas:

- Manual: La dirección IP se introduce mediante el teclado o cualquier otro dispositivo que lo permita.
- Automáticamente: El servidor DHCP (Dynamic Host Configuration Protocol), asigna siempre la misma IP a un dispositivo.
- Dinámicamente: El servidor DHCP asigna una IP del rango de direcciones que tiene disponible, la dirección IP puede coincidir.

Ejercicios

Crear una función en la que le pasas una conexión de red y te dice qué proceso ejecuta (le puedes pasar una IP o un puerto)

- https://www.jesusninoc.com/02/09/ejercicios-de-powershell-crear-una-funcion-en-la-que-se-pasa-una-conexion-de-red-y-te-dice-proceso-ejecuta-se-puede-pasar-una-ip-o-un-puerto/

Crear una función que agrupa los nombre obtenidos mediante una resolución DNS (sin mostrar errores)

- https://www.jesusninoc.com/02/09/ejercicios-de-powershell-crear-una-funcion-que-agrupa-los-nombre-obtenidos-mediante-una-resolucion-dns-sin-mostrar-errores/

Mostrar los hilos que se están ejecutando y deducir si se pueden relacionar con sockets abiertos

- https://www.jesusninoc.com/02/09/ejercicios-de-powershel

l-mostrar-los-hilos-que-se-estan-ejecutando-y-deducir-si-se-pueden-relacionar-con-sockets-abiertos-tcp-o-udp/

Optimización de sistemas para ordenadores portátiles. Archivos de red sin conexión

En este apartado se describe cómo deshabilitar el almacenamiento en caché de Archivos sin conexión en carpetas individuales que se redirigen a recursos compartidos de red mediante Redirección de carpetas. Este proceso permite especificar las carpetas que se excluirán del almacenamiento en caché de forma local, lo que reduce el tamaño de la caché de Archivos sin conexión y el tiempo necesario para sincronizar Archivos sin conexión.

Ejemplos

Enable the Microsoft Windows Firewall

- https://www.jesusninoc.com/2016/05/16/enable-the-microsoft-windows-firewall/

Disable the Microsoft Windows Firewall

- https://www.jesusninoc.com/2016/05/15/disable-the-microsoft-windows-firewall/

Reglas de firewall

- https://www.jesusninoc.com/02/09/mostrar-las-reglas-del-firewall-de-windows-desde-powershell-que-estan-habilitadas/
- https://www.jesusninoc.com/02/09/mostrar-las-reglas-del-

firewall-de-windows-desde-powershell-que-estan-deshabilitadas/

- https://www.jesusninoc.com/02/09/mostrar-las-reglas-del-firewall-en-windows-desde-powershell-que-estan-habilitadas-y-permiten-conexion/
- https://www.jesusninoc.com/02/09/mostrar-las-reglas-del-firewall-de-windows-desde-powershell-que-estan-habilitadas-y-no-permiten-conexion/
- https://www.jesusninoc.com/02/09/mostrar-los-puertos-que-estan-abiertos-en-las-reglas-del-firewall-de-windows-desde-powershell-que-estan-habilitadas-y-permiten-conexion/
- https://www.jesusninoc.com/02/09/mostrar-los-puertos-que-estan-abiertos-en-las-reglas-de-salida-del-firewall-desde-powershell-de-windows-que-estan-habilitadas-y-permiten-conexion/
- https://www.jesusninoc.com/02/09/mostrar-los-puertos-que-estan-abiertos-en-las-reglas-de-entrada-del-firewall-de-windows-desde-powershell-que-estan-habilitadas-y-permiten-conexion/
