uso: pywerview [-h]

{get-adobject,get-objectacl,get-netuser,get-netgroup,get-netcomputer,get-netdomaincontroller,get-netfileserver,get-dfsshare,get-netou,get-netsite,get-netsubnet,get-netdomaintrust,get -netgpo,get-netpso,get-domainpolicy,get-gpttmpl,get-netgpogroup,find-gpocomputeradmin,find-gpolocation,get-netgroupmember,get-netsession,get-localdisks,get-netdomain,get-netshare,get-netloggedon ,get-netlocalgroup,invoke-checklocaladminaccess,get-netprocess,get-userevent,invoke-userhunter,invoke-processhunter,invoke-eventhunter}

...

Reescritura de algunas funcionalidades de PowerView en Python

opciones:

-h, --help muestra este mensaje de ayuda y sale

Subcomandos:

Subcomandos disponibles

{get-adobject,get-objectacl,get-netuser,get-netgroup,get-netcomputer,get-netdomaincontroller,get-netfileserver,get-dfsshare,get-netou,get-netsite,get-netsubnet,get-netdomaintrust,get -netgpo,get-netpso,get-domainpolicy,get-gpttmpl,get-netgpogroup,find-gpocomputeradmin,find-gpolocation,get-netgroupmember,get-netsession,get-localdisks,get-netdomain,get-netshare,get-netloggedon ,get-netlocalgroup,invoke-checklocaladminaccess,get-netprocess,get-userevent,invoke-userhunter,invoke-processhunter,invoke-eventhunter}

get-adobject Toma un SID de dominio, samAccountName o nombre, y devuelve el objeto asociado

get-objectacl Toma un SID de dominio, samAccountName o nombre, y devuelve la ACL del objeto asociado.

get-netuser Consulta información sobre un usuario de dominio

get-netgroup Obtenga una lista de todos los grupos de dominio actuales, o una lista de grupos de los que es miembro un usuario de dominio.

get-netcomputer Consulta información sobre las computadoras del dominio

get-netdomaincontroller

Obtenga una lista de controladores de dominio para el dominio determinado

get-netfileserver Devuelve una lista de servidores de archivos, extraída del directorio de inicio, ruta de script y ruta de perfil de los usuarios del dominio.

campos

get-dfsshare Devuelve una lista de todos los sistemas de archivos distribuidos tolerantes a fallos para un dominio determinado

get-netou Obtenga una lista de todas las unidades organizativas actuales en el dominio

get-netsite Obtenga una lista de todos los sitios actuales en el dominio

get-netsubnet Obtenga una lista de todas las subredes actuales en el dominio

get-netdomaintrust Devuelve una lista de todas las confianzas del dominio especificado

get-netgpo Obtenga una lista de todos los GPO actuales en el dominio

get-netpso Obtenga una lista de todos los PSO actuales en el dominio

get-domainpolicy Devuelve el dominio predeterminado o la política de DC para el dominio o DC consultado

get-gpttmpl Ayuda para analizar la ruta del archivo de política GptTmpl.inf en un objeto personalizado

get-netgpogroup Analiza todos los GPO en el dominio que configuran "Grupo restringido" o "Grupos.xml"

encontrar-gpocomputeradmin

Toma una computadora (u OU) y determina quién tiene acceso administrativo a ella a través de GPO

find-gpolocation Toma un nombre de usuario o un nombre de grupo y determina las computadoras a las que tiene acceso administrativo a través de GPO

get-netgroupmember Devuelve una lista de miembros de un grupo de dominio

get-netsession Consulta un host para devolver una lista de sesiones activas en el host (puede usar credenciales locales en lugar de

credenciales de dominio)

get-localdisks Consulta un host para devolver una lista de discos activos en el host (puede usar credenciales locales en lugar de

credenciales de dominio)

get-netdomain Consulta un host sobre dominios disponibles

get-netshare Consulta un host para devolver una lista de recursos compartidos disponibles en el host (puede usar credenciales locales en lugar de

credenciales de dominio)

get-netloggedon Esta función ejecutará la llamada RPC NetWkstaUserEnum para consultar en un host determinado los usuarios que han iniciado sesión activamente.

get-netlocalgroup Obtiene una lista de miembros de un grupo local en una máquina o devuelve cada grupo local. Puedes usar locales

credenciales en lugar de credenciales de dominio; sin embargo, se necesitan credenciales de dominio para resolver los SID de dominio.

invocar-checklocaladminaccess

Comprueba si el usuario determinado tiene acceso de administrador local en el host determinado

get-netprocess Esta función ejecutará la consulta WMI 'Seleccionar \* de Win32\_Process' a un host determinado para obtener una lista de

proceso ejecutado

get-userevent Esta función ejecutará la consulta WMI 'Seleccionar \* de Win32\_Process' a un host determinado para obtener una lista de

proceso ejecutado

invoke-userhunter Encuentra en qué máquinas están conectados los usuarios del dominio

cazador de procesos de invocación

Busca en las máquinas procesos con un nombre específico o ejecutados por usuarios específicos

invoke-eventhunter Busca en las máquinas eventos con un nombre específico o ejecutados por usuarios específicos