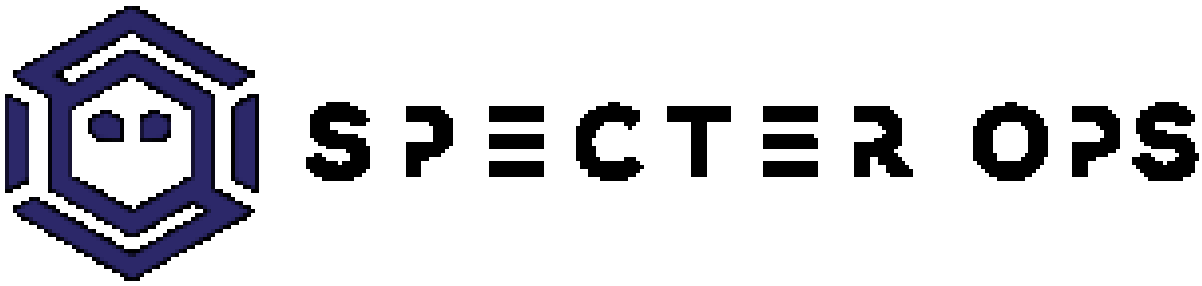

# Шпаргалка по PowerView 3.0

## Начало работы

Внимание: важные обновления PowerView **всегда** будут находиться в ветке разработки PowerSploit: **http://bit.ly/1pzQCnv**

Загрузка с диска:

1) `C:\> powershell -exec bypass`
2) `PS C:\> Import-Module powerview.ps1`

Запуск на устройстве не из доменной зоны:

1) `configure DNS to point to DC of domain`
2) `runas /netonly/user:DOMAIN\user powershell.exe`

Загрузка через Cobalt Strike Beacon:

1) `beacon> powershell- import /local/path/to/PowerView.ps1`
2) `beacon> powershell CMDLET-NAME`

Помощь и дополнительная информация: `PS C:\> Get-Help Cmdlet-Name [-detailed]`

## Фильтрация и вывод

| | |
|---|---|
| Выполнение команды в отношении каждого объекта из результатов | `… \| %{…Invoke- Command $_ }` |
| Фильтрация результатов по полю | `… \| ? {$_.Field -eq X}` |
| Вывод только определённых свойств | `… \| Select prop1,prop2` |
| Отображение результатов в виде списка | `… \| fl` |
| Отображение результатов в виде «обёрнутой» таблицы | `… \| ft -wrap` |
| Запись в файл | `… \| Out-File -Encoding Ascii out.txt` |
| Запись в .csv | `… \| Export-CSV - NoTypeInformation out.csv` |
| Запись в объект .xml | `…\| Export-Clixml obj.xml` |

| | |
|---|---|
| Чтение объекта .xml | `$obj = Import-Clixml obj.xml` |

## Схема именования функций

Все функции PowerView теперь следуют правильному формату **Verb-PrefixNoun**:

| | |
|---|---|
| `Get-*` | Запрос полных объектов необработанных данных |
| `Find-*` | Поиск определённых записей в наборе данных или выполнение перечисления потоковых устройств |
| `Add-*` | Добавление нового объекта в место назначения |
| `Set-*` | Изменение данного объекта |
| `Invoke-*` | Lazy catch-all - ??? |

Именные префиксы теперь дают определение источнику данных:

| | |
|---|---|
| `Verb-DomainX` | LDAP/.NET AD-соединения |
| `Verb-WMIX` | Использование WMI для соединения/перечисления |
| `Verb-NetX` | Использование API-вызовов Win32 |

## Общие функции

| | |
|---|---|
| Объект для запроса – samaccountname, DN, SID, GUID или dnsHostname. Как аргумент принимаются подстановочные знаки. | `-Identity <X>` |
| Отображение подробной информации о состоянии/отладке | `-Verbose` |
| Выполнение запроса в чужом домене | `-Domain foreign.com` |
| Использование настраиваемого LDAP-фильтра | `-LDAPFilter '(prop- value)'` |
| Вывод только указанные свойств с сервера | `-Properties prop1,prop2` |
| Поиск по определённому OU | `-SearchBase "ldap://OU=…"` |
| Поиск в глобальном каталоге | `-SearchBase "GC://domain.com"` |
| Привязка к определённому серверу для поиска | `-Server "dc.domain.com"` |
| Вывод определённой информаций безопасности с помощью поиска | `-SecurityMasks [Dacl/Owner/Sacl]` |
| Вывод только одного результата | `-FindOne` |

## -Credential

Все функции PowerView теперь принимают альтернативное уточнение `-Credential` specification:

- `PS C:\> $SecPassword = ConvertTo-SecureString 'BurgerBurgerBurger!' -AsPlainText -Force`
- `PS C:\> $Cred = New-Object System.Management.Automation.PSCredential('TESTLAB\dfm.a', $SecPassword)`
- `PS C:\> Get-DomainUser -Credential $Cred`

## Перечисление устройств

`Get-DomainComputer` перечислит объекты *computer* на данном домене через LDAP.

| | |
|---|---|
| Вывод только активных хостов | `-Ping` |
| Устройства с неограниченным делегированием | `-Unconstrained` |
| Есть право аутентифицировать других участников | `-TrustedToAuth` |
| Определённое имя участника службы, как аргументы принимаются подстановочные знаки | `-SPN *SQL*` |
| Определённая ОС, как аргументы принимаются подстановочные знаки | `-OperatingSystem <X>` |
| Определённый сервис-пак, как аргументы принимаются подстановочные знаки | `-ServicePack <X>` |

## Определение вашей жертвы

`Get-DomainUser` перечислит объекты *user* на данном домене через LDAP.

| | |
|---|---|
| Вывод пользователей с “admin” в имени | `-Identity “*john*”` |
| Вывод пользователей, состоящих/состоявших в защищённой группе администраторов | `-AdminCount` |
| Пользователи с набором имён участников службы (вероятные служебные аккаунты) | `-SPN` |
| Есть право аутентифицировать других участников | `-TrustedToAuth` |
| Установлено “Не запрашивать Kerberos preauthentication” | `-PreauthNotRequired` |

`Get-DomainGroup` перечислит объекты *group* на данном домене через LDAP.

| | |
|---|---|
| Вывод групп с “admin” в имени группы | `-Identity *admin*` |
| Вывод групп, к которым принадлежит конкретный пользователь/группа | `-MemberIdentity <X>` |
| Вывод привилегированных групп | `-AdminCount` |
| Вывод групп в определённом масштабе | `-GroupScope [DomainLocal/Global/Universal]` |

`Get-DomainGroupMember` перечислит *members* (членов) определённой группы на данном домене через LDAP.

| | |
|---|---|
| Определённое название группы | `-Identity "Domain Admins"` |
| Рекурсивное разрешение любых членов результата, которые являются группами | `-Recurse` |

Если вы не уверены, какой у объекта тип, можно использовать `Get-DomainObject`. `Get-DomainObjectACL` выведет все ACL, ассоциированные с определённым объектом active directory**.** Флаг `-ResolveGUIDs` добавляет ACE GUID в отображаемые имена.

## Домены [Trusts]

| | |
|---|---|
| Информация о текущем лесе доменов | `Get-Forest` |
| Перечисление всех доменов текущего леса | `Get-ForestDomain` |
| Получение всех трастов текущего леса | `Get-ForestTrust` |
| Информация текущего домена | `Get-Domain` |
| Получение всех трастов домена (аналог **nltest/trusted_domains**) | `Get-DomainTrust` |
| Рекурсивная разметка всех трастов домена | `Get-DomainTrustMapping` |
| Поиск пользователей в группах вне текущего домена (исходящий доступ) | `Get-DomainForeignUser` |
| Поиск групп с пользователями вне текущего домена (входящий доступ) | `Get- DomainForeignGroupMember` |

Все функции `Verb-Domain*` также принимают `-Domain <X>` для запроса определённой информации из внешнего домена.

## Поиск пользователей

`Find-DomainUserLocation` (ранее `Invoke-UserHunter`) использует LDAP-запросы и API-вызовы для определения пользователей домена. Внимание: с настройками по умолчанию эта команда ищет "Domain Admins" и затронет все устройства на домене!

| | |
|---|---|
| Задаёт одного или более *user* для поиска | `-UserIdentity <X>` |
| Задаёт хосты для перечисления для получения информации о сессии | `-ComputerName X,Y` |
| Задаёт одну или более *groups* для запроса поиска пользователей | `-UserGroupIdentity <X>` |
| Отображение всех результатов (то есть, не применять фильтры) | `-ShowAll` |

| | |
|---|---|
| Искать на файловых серверах и DC только информацию о сессиях | `-Stealth` |
| Проверка, имеет ли текущий пользователь доступ администратора на устройствах, где найдены целевые пользователи | `-CheckAccess` |

## Получение данных

`Find-DomainShare` (ранее – `Invoke-ShareFinder`) использует LDAP-запросы и API-вызовы для поиска открытых share'ов на домене. Внимание: с настройками по умолчанию эта команда затронет все устройства на домене!

| | |
|---|---|
| Вывод только тех share'ов, которые может прочитать текущий пользователь | `-CheckShareAccess` |
| Вывод только тех share'ов, которые находятся на устройствах в заданном OU | `-ComputerSearchBase "ldap://OU=…"` |

`Find-InterestingFile` производит рекурсивный поиск файлов в указанном локальном или UNC пути на соответствие заданным критериям.

| | |
|---|---|
| Поиск указанного пути UNC | `-Path \\SERVER\Share` |
| Вывод файлов только с заданными частями в именах файлов | `-Include term1,term2,term3` |
| Вывод только документов | `-OfficeDocs` |
| Вывод файлов, которые использовались в течение недели | `-LastAccessTime (Get-Date).AddDays(-7)` |

## Перечисление локальных администраторов

`Get-NetLocalGroupMember` перечисляет локальных пользователей и группы из localhost или удалённых устройств.

| | |
|---|---|
| Перечисление локальных администраторов из hostname (или IP) | `-ComputerName <X>` |
| Использование альтернативной группы помимо локальных администраторов | `-GroupName "Remote Desktop Users"` |
| Использование провайдера служб WinNT (по умолчанию) или API-вызовы Win32 | `-Method [WinNT/API]` |

## Дополнительные функции

| | |
|---|---|
| Вывод OU домена | `Get-DomainOU` |

| | |
|---|---|
| Вывод GPO домена | `Get-DomainGPO` |
| Поиск вероятных файловых серверов, основываясь на свойствах пользователя | `Get-DomainFileServer` |
| Перечисление share'ов на определённом устройстве | `Get-NetShare <X>` |
| Перечисление share'ов на определённом устройстве | `Get-NetSession <X>` |
| Перечисление RDP-сессий (и IP-адресов источников) | `Get-NetRDPSession <X>` |

## Дополнительная информация

- Последнее обновление: http://bit.ly/2rseIm6
- Хитрости PowerView – http://bit.ly/2tDBAQi
- http://www.harmj0y.net/blog/tag/powerview/
- https://specterops.io