Как выбрать подходящий exec-скрипт в Impacket

spy-soft.net/impacket-exec

29 августа 2024 г.

Хочешь научится пентестить (взламывать) компьютеры, изучи Impacket! Когда я впервые столкнулся с этой тулзой, то с удивлением обнаружил множество скриптов, заканчивающихся на exec. Каждый из них предоставляет удаленный доступ, но возникает вопрос: когда, какой использовать? Если ты в такой же ситуации, не волнуйся, я тебе помогу в выборе и использовании скриптов Impacket.

Еще по теме: Реальный пример проведения пентеста

Что такое Impacket

Impacket — это набор инструментов и библиотек на Python, который позволяет работать с сетевыми протоколами и выполнять атаки на сетевом уровне, например, осуществлять перебор паролей, манипулировать сетевыми пакетами, инициализировать сессии и выполнять команды на удаленных системах. Он широко используется для тестирования на проникновение и анализа безопасности.

Мы о нем рассказывали в статье «Лучшие библиотеки Python для хакеров».

Exec скрипты в Impacket

Exec-скрипты в Impacket — это инструменты для удаленного выполнения команд на целевых системах через различные протоколы и методы, такие как SMB, WMI и DCOM. Они позволяют получить удаленный доступ к системе, создавая службы, выполняя задачи или взаимодействуя с системными компонентами.

> Все методы описанные в этой статье, предназначены для обучения пентестеров (этичных хакеров). Использование данных скриптов для атак на частные лица или организации без их предварительного согласия является незаконным. Ни редакция spy-soft.net, ни автор не несут ответственности за ваши действия.

Эти скрипты включают PsExec, SmbExec, WmiExec, AtExec и DcomExec, и каждый из них используется в зависимости от контекста и требований безопасности.

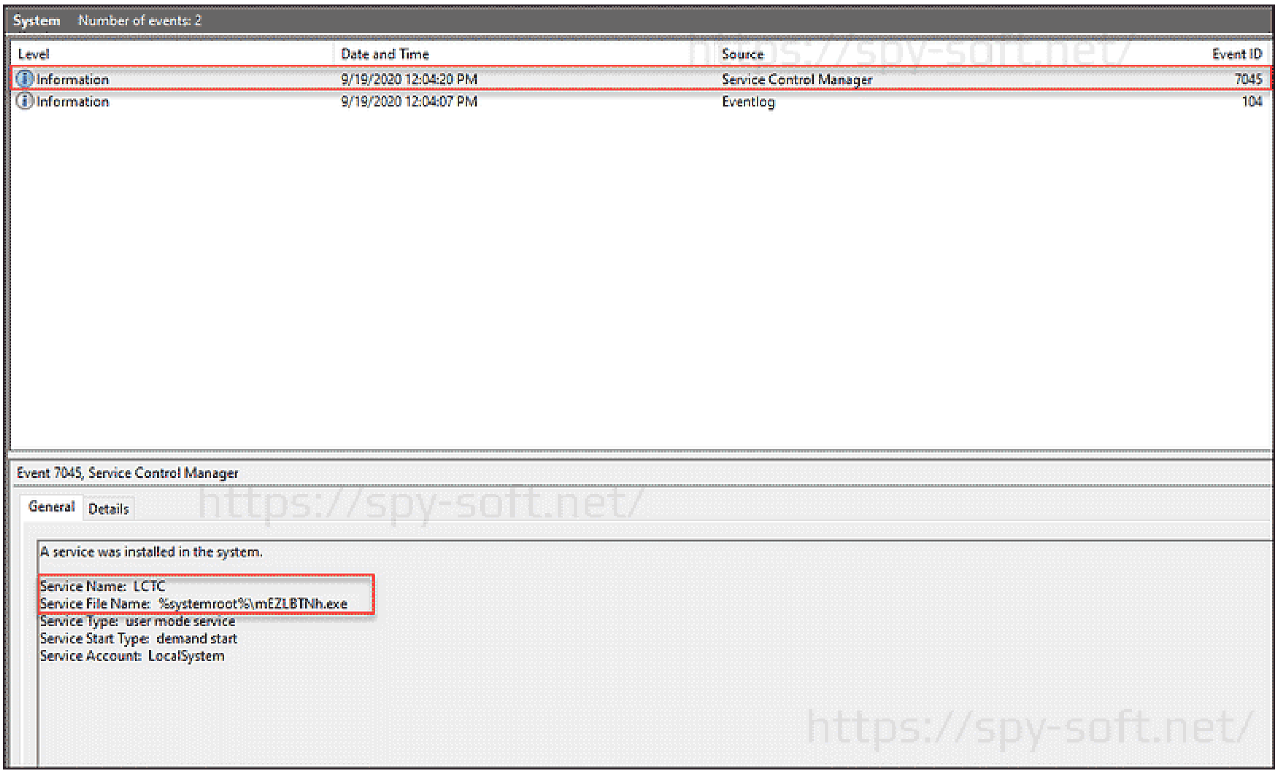
PsExec

PsExec работает, записывая бинарник со случайным именем в SMB-шару ADMIN$ (поэтому для его использования тебе нужно иметь права на запись в эту шару). Файл, для создания новой службы, устанавливает канал связи, который используется SVCManager. Его можно юзать для удаленного выполнения команд. По сути, это похоже на выполнение следующей команды:

```
sc create [serviceName] binPath= "C:\Windows\[uploaded-binary].exe"
```

Ввод и вывод команд происходит через канал связи по протоколу SMB (445/TCP).

PsExec оставляет артефакты, которые нужно вручную удалять, так как загруженный файл не удаляется автоматически. Вот как выглядят журналы Windows после выполнения одной команды через PsExec:



System Number of events: 2

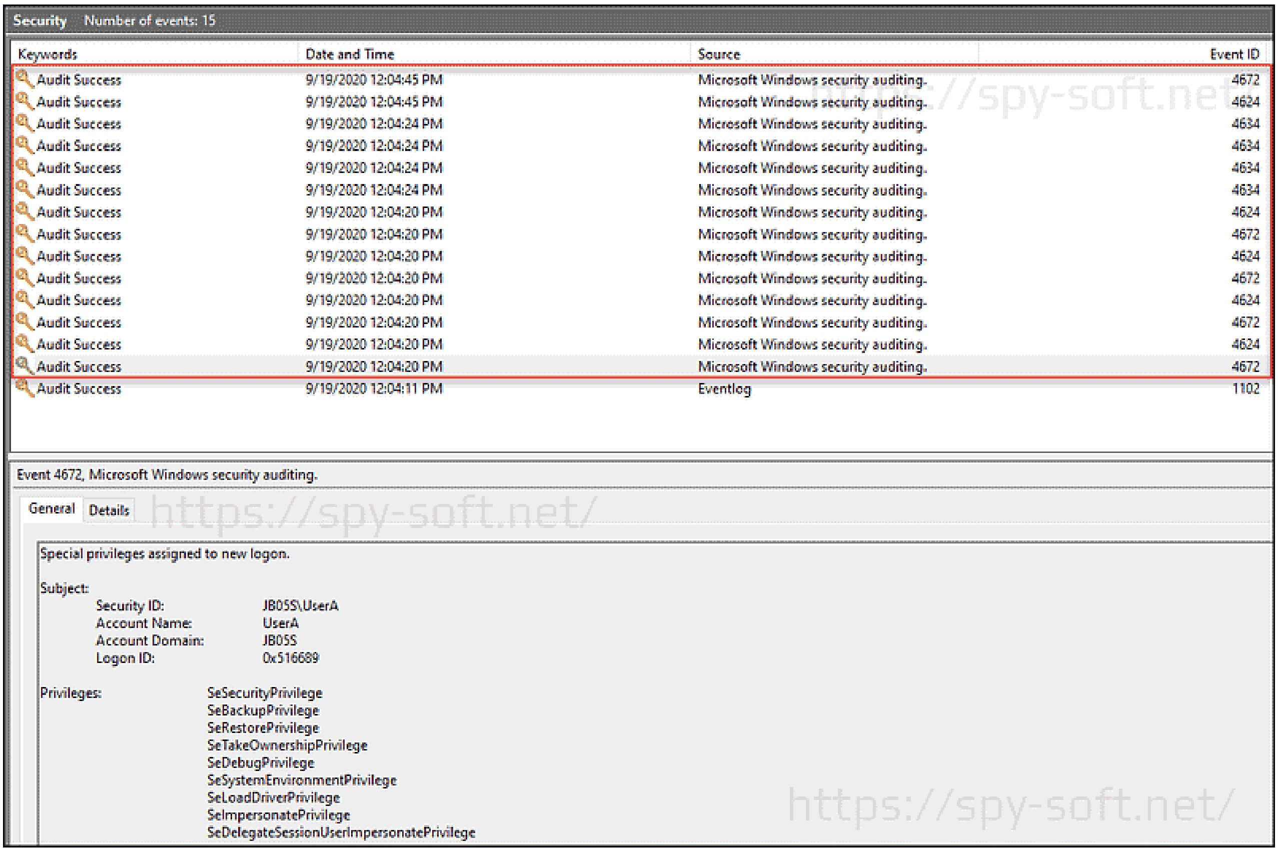
Level	Date and Time	Source	Event ID
Information	9/19/2020 12:04:20 PM	Service Control Manager	7045
Information	9/19/2020 12:04:07 PM	Eventlog	104

Event 7045, Service Control Manager

```
A service was installed in the system.

Service Name:  LCTC
Service File Name:  %systemroot%\mEZLBTNh.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Журнал ошибок Windows



Security Number of events: 15

Keywords	Date and Time	Source	Event ID
Audit Success	9/19/2020 12:04:45 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:04:45 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:04:24 PM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 12:04:24 PM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 12:04:24 PM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 12:04:24 PM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:04:20 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:04:11 PM	Eventlog	1102

Event 4672, Microsoft Windows security auditing.

```
Special privileges assigned to new logon.

Subject:
        Security ID:        JB05S\UserA
        Account Name:       UserA
        Account Domain:     JB05S
        Logon ID:           0x516689

Privileges:             SeSecurityPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeTakeOwnershipPrivilege
                        SeDebugPrivilege
                        SeSystemEnvironmentPrivilege
                        SeLoadDriverPrivilege
                        SeImpersonatePrivilege
                        SeDelegateSessionUserImpersonatePrivilege
```

Журнал безопасности Windows

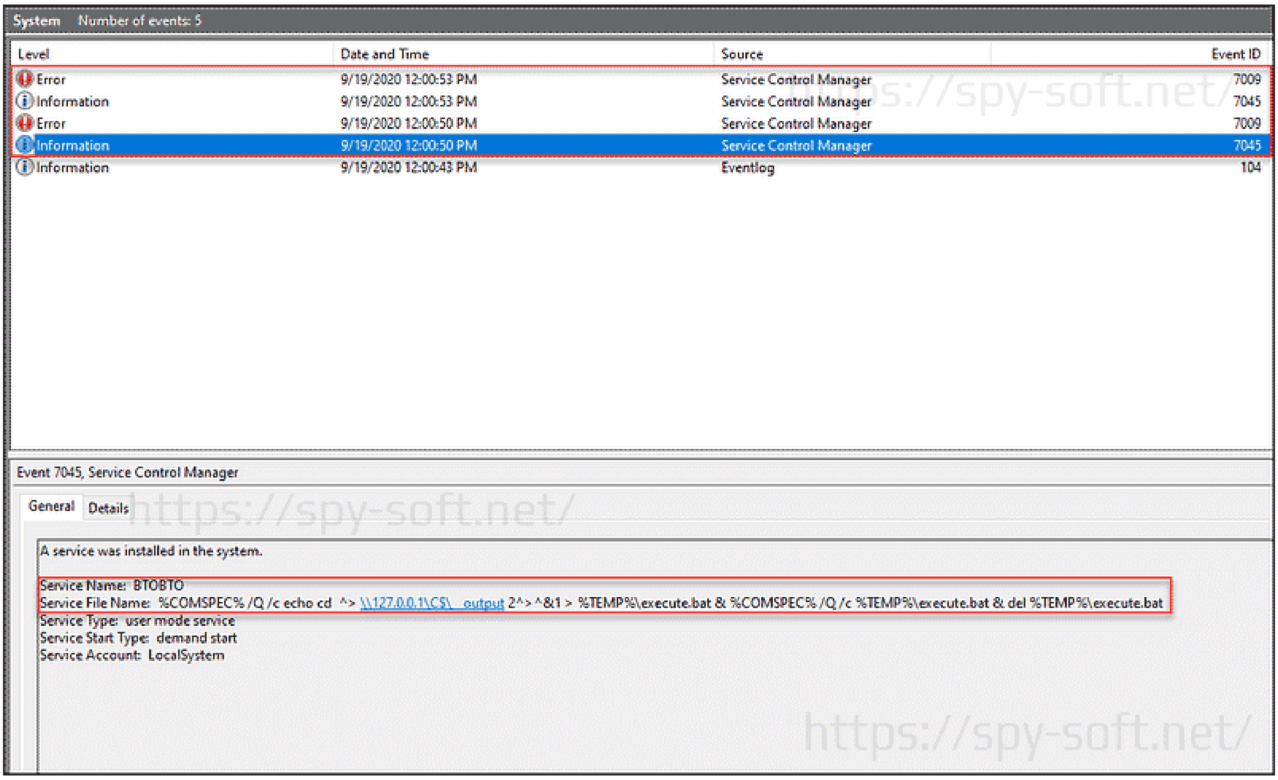
В журналах отображаются следующие события:

- 1 системное событие с ID 7045 (Запуск службы)
- 12 событий безопасности с ID 4672 (Специальный вход с привилегиями), 4624 (Вход в систему), 4634 (Выход из системы)

SmbExec

SmbExec работает аналогично PsExec. Основное различие в том, что PsExec загружает .exe файл в шару ADMIN$, а SmbExec загружает .bin файл вместе с временным файлом.

Вот следы, которые остаются в журналах после установления соединения через SmbExec, выполнения команды и выхода:



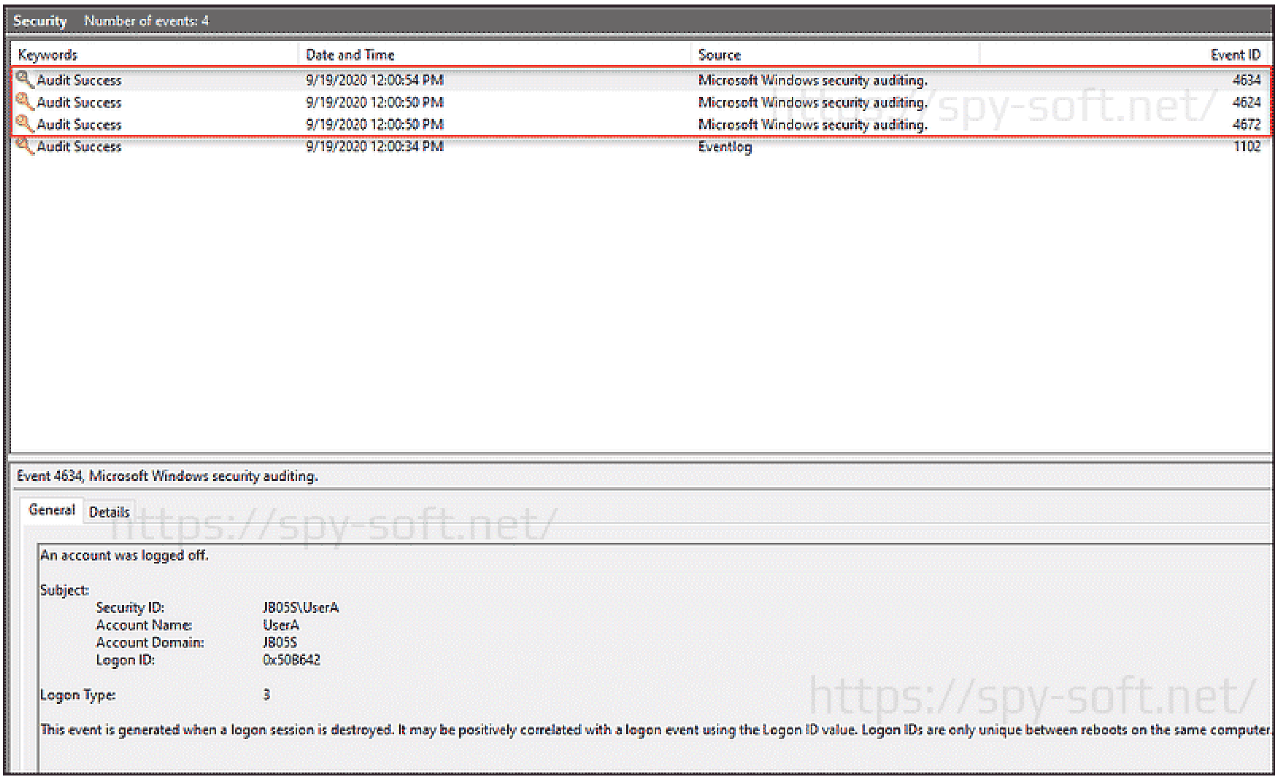
Level	Date and Time	Source	Event ID
Error	9/19/2020 12:00:53 PM	Service Control Manager	7009
Information	9/19/2020 12:00:53 PM	Service Control Manager	7045
Error	9/19/2020 12:00:50 PM	Service Control Manager	7009
Information	9/19/2020 12:00:50 PM	Service Control Manager	7045
Information	9/19/2020 12:00:43 PM	Eventlog	104

```
Event 7045, Service Control Manager

A service was installed in the system.

Service Name:  BTOBTO
Service File Name:  %COMSPEC% /Q /c echo cd  ^> \\127.0.0.1\C$\__output 2^> ^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Журнал ошибок Windows



Keywords	Date and Time	Source	Event ID
Audit Success	9/19/2020 12:00:54 PM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 12:00:50 PM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 12:00:50 PM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 12:00:34 PM	Eventlog	1102

```
Event 4634, Microsoft Windows security auditing.

An account was logged off.

Subject:
        Security ID:        JB05S\UserA
        Account Name:       UserA
        Account Domain:     JB05S
        Logon ID:           0x50B642

Logon Type:                 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
```

Журнал безопасности Windows

В результате в журналах отображаются:

- 4 системных события с ID 7045 (Запуск службы), 7009 (Ошибка службы — тайм-аут)
- 3 события безопасности с ID 4672 (Специальный вход с привилегиями), 4624 (Вход в систему), 4634 (Выход из системы)

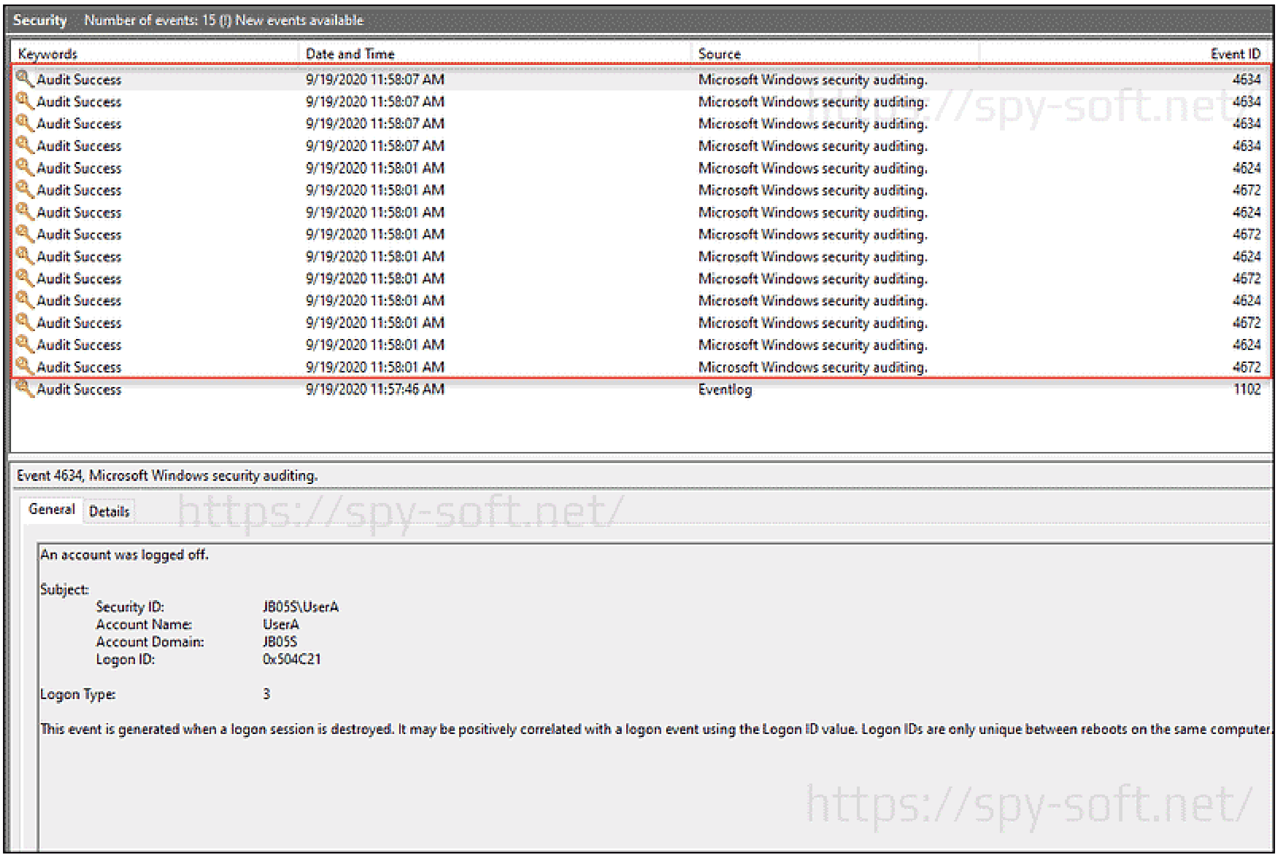
Wmiexec или Psexec

Wmiexec работает через Windows Management Instrumentation (WMI). WMI использует случайный порт (>1024), устанавливая начальное соединение через RCP (135/TCP). WMI и RPC часто используются для управления сетями, поэтому порты часто открыты и не фильтруются во внутренних сетях.

Пользователь отправляет команды на удаленный хост через случайный порт. Команды выполняются с помощью cmd.exe, а вывод записывается в файл в SMB-шаре ADMIN$. Имя файла начинается с двух подчеркиваний, за которыми следует временная метка.

Преимущество этого метода в том, что он позволяет выполнять код без записи на диск, что снижает вероятность обнаружения. Кроме того, WMI можно использовать для удаленного доступа через тулзу pth-wmis, которая предустановлена в Kali Linux.

Журналы после установления соединения через Wmiexec, выполнения команды и выхода выглядят таким образом:



Security Number of events: 15 (!) New events available

Keywords	Date and Time	Source	Event ID
Audit Success	9/19/2020 11:58:07 AM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 11:58:07 AM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 11:58:07 AM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 11:58:07 AM	Microsoft Windows security auditing.	4634
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4624
Audit Success	9/19/2020 11:58:01 AM	Microsoft Windows security auditing.	4672
Audit Success	9/19/2020 11:57:46 AM	Eventlog	1102

Event 4634, Microsoft Windows security auditing.

```
An account was logged off.

Subject:
        Security ID:            JB05S\UserA
        Account Name:           UserA
        Account Domain:         JB05S
        Logon ID:               0x504C21

Logon Type:                     3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
```

Журнал событий Windows

В журналах отображаются:

- 14 событий безопасности с ID 4672 (Специальный вход с привилегиями), 4624 (Вход в систему), 4634 (Выход из системы)

AtExec

Этот инструмент работает через удаленное выполнение запланированных задач на целевой системе через RCP. Она создает задачу с помощью службы планировщика задач. Задача выполняется через cmd.exe, а вывод команды (STDERR и STDERR) записывается во временный файл в SMB-шаре ADMIN$. AtExec извлекает данные из этого файла перед его удалением.

DcomExec

Эта программа использует протокол DCOM. DCOM сильно полагается на RPC для взаимодействия программных компонентов на сетевых компьютерах. У нее такой же интерфейс, как у PsExec, и она работает следующим образом:

Dcomexec использует приложение MMC20 (доступное по сети при наличии аутентификации) и его метод ExecuteShellCommand для выполнения произвольных команд. Также поддерживается использование приложений ShellWindows и ShellBrowserWindow.

Заключение

Суммируем всю информацию в небольшую шпаргалку:

- **PsExec** работает через SMB, загружая .exe файл, который создает канал между тобой и удаленным хостом.
- **SmbExec** работает аналогично, но использует .bin файл вместо .exe.
- **Wmiexec** использует службу Windows Management Instrumentation для отправки команд на хост, а вывод записывается в файл в SMB.
- **AtExec** работает через выполнение запланированных задач в SMB.
- **DcomExec** для выполнения команд использует протокол DCOM с RPC.

Все эти инструменты оставляют различные следы в журналах, и при пентесте надо это учитывать.

На этом все. Надеюсь, тебе было интересно, потому что я сам узнал много нового.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Локальная альтернатива Sysinternals PsExec.exe
- Атака Pass the Hash с помощью PsExec Impacket