Просмотр и анализ логов RDP подключений в Windows

http://winitpro.ru/index.php/2018/09/25/analizing-rdp-logs-windows-terminal-rds/

В этой статье мы рассмотрим, особенности аудита / анализа логов RDP подключений в Windows. Как правило, описанные методы могут пригодиться при расследовании различных инцидентов на терминальных / RDS серверах Windows, когда от системного администратора требуется предоставить информацию: какие пользователи входили на RDS сервер, когда авторизовался и завершил сеанс конкретный пользователь, откуда / с какого устройства (имя или IP адрес) подключался RDP-пользователь. Я думаю, эта информация будет полезна как для администраторов корпоративных RDS ферм, так и владельцам RDP серверов в интернете (Windows VPS как оказалось довольно популярны).

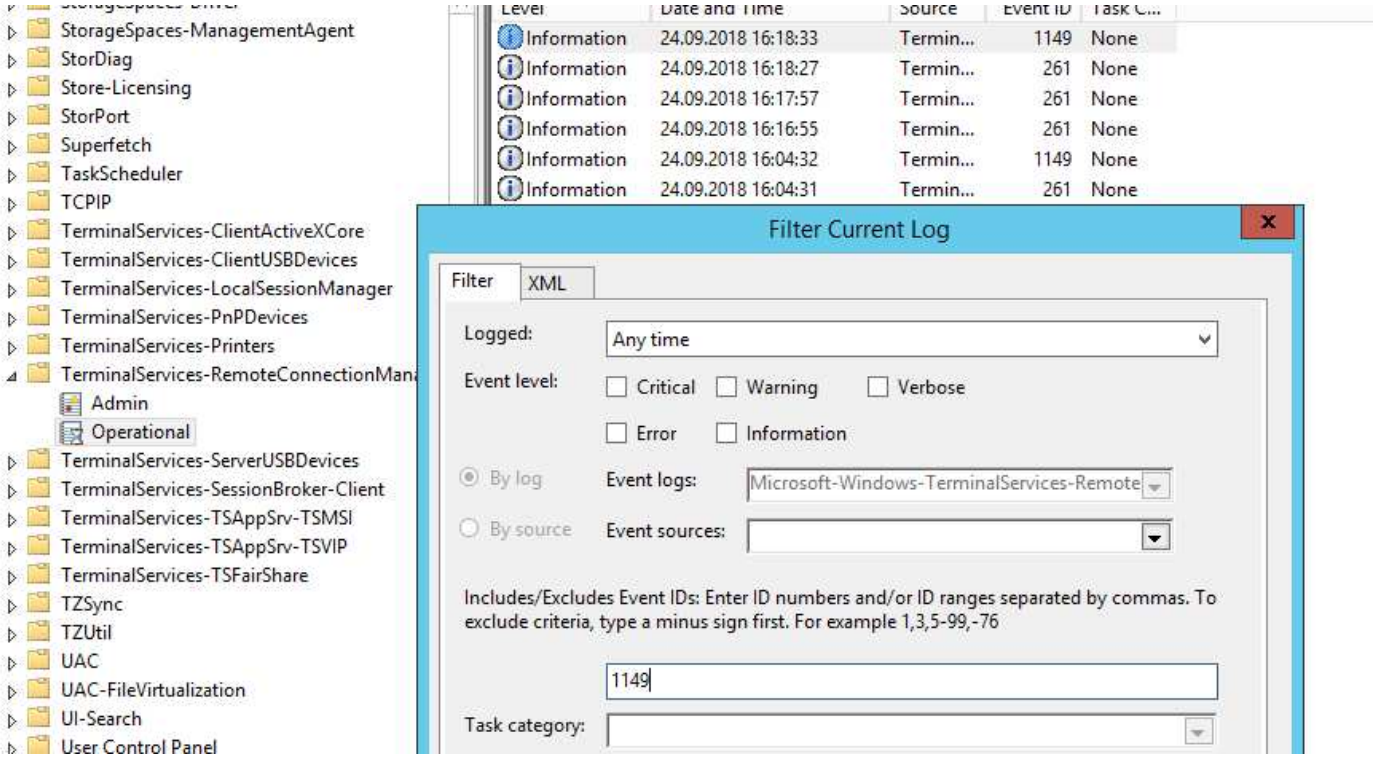
Статья применима при исследовании RDP логов как в Windows Server 2008 R2, 2012/R2, 2016, так и в соответствующих десктопных версиях Windows (Windows 7, 8.1, 10).

Как и другие события, логи RDP подключения в Windows хранятся в журналах событий. Откройте консоль журнала событий (Event Viewer). Есть несколько различных журналов, в которых можно найти информацию, касающуюся RDP подключения.

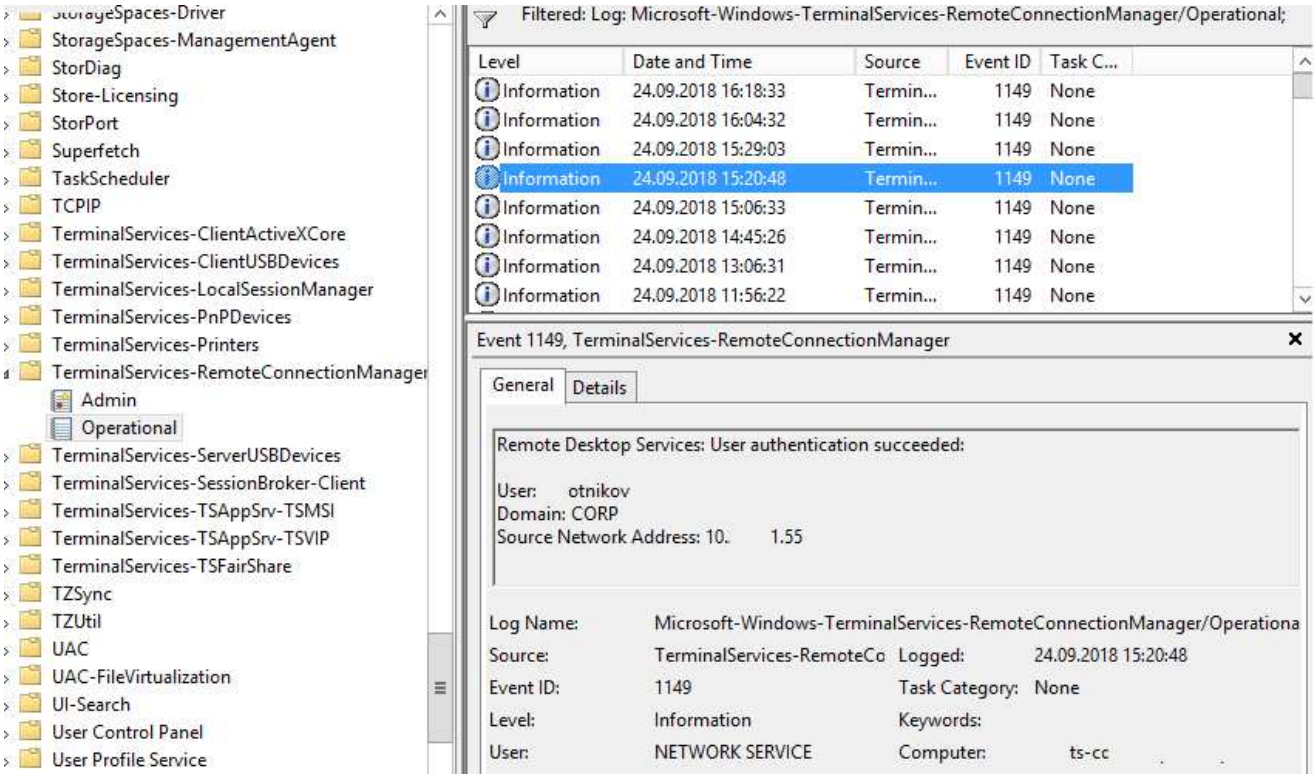
В журналах Windows содержится большое количество информации, но быстро найти нужное событие бывает довольно сложно. Когда пользователь удаленно подключается к RDS серверу или удаленному столу (RDP) в журналах Windows генерируется много событий. Мы рассмотрим журналы и события на основных этапах RDP подключения, которые могут быть интересны администратору:

1. **Network Connection**
2. **Authentication**
3. **Logon**
4. **Session Disconnect/Reconnect**
5. **Logoff**

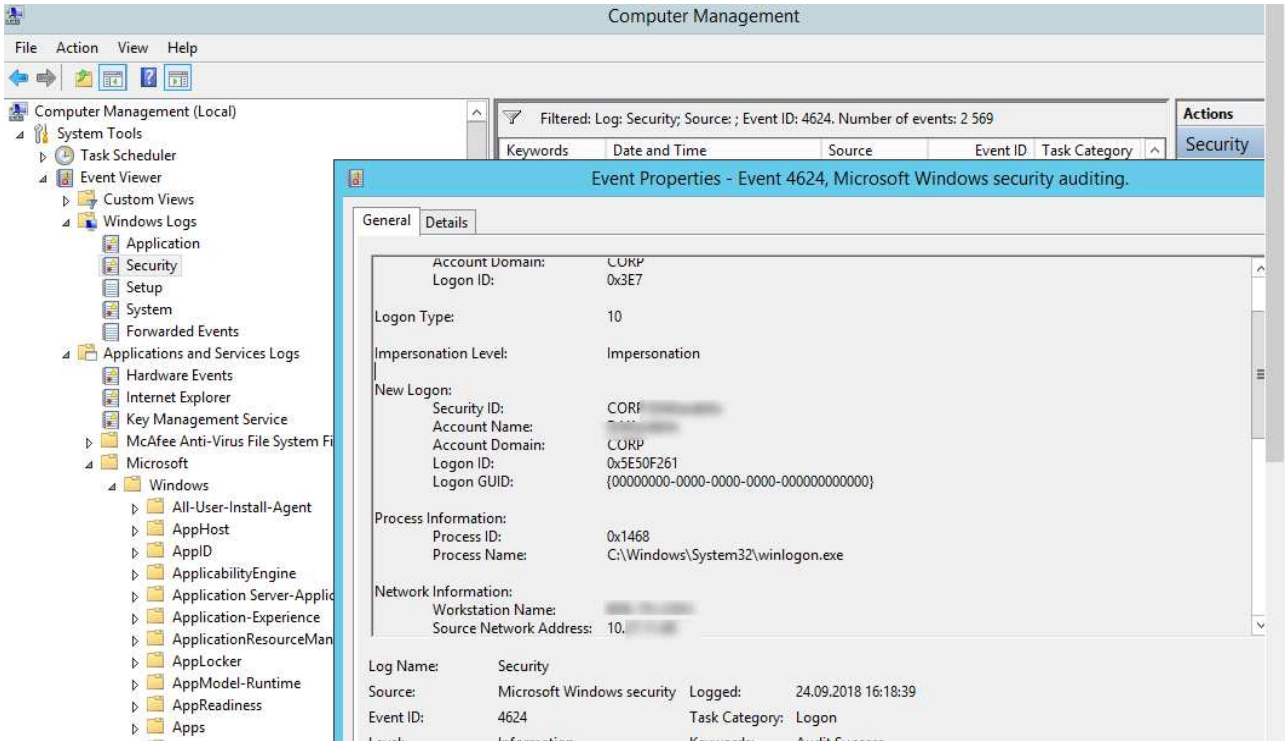
1. **Network Connection:** – установление сетевого подключение к серверу от RDP клиента пользователя. Событие с EventID – **1149 (**Remote Desktop Services: User authentication succeeded**)**. Наличие этого события не свидетельствует об успешной аутентификации пользователя. Этот журнал находится в разделе Applications and Services Logs -> Microsoft -> Windows -> **Terminal-Services-RemoteConnectionManager** -> Operational. Включите фильтр по данному событию (ПКМ по журналу-> Filter Current Log -> **EventId 1149**).



В результате у вас получится список с историей всех сетевых RDP подключений к данному серверу. Как вы видите, в логах указывается имя пользователя, домен (используется NLA аутентификация, при отключенном NLA текст события выглядит иначе) и IP адрес компьютера, с которого осуществляется RDP подключение.



2. **Authentication:** – успешная или неуспешная аутентификация пользователя на сервере. Журнал Windows -> Security. Соответственно нас могут интересовать события с **EventID – 4624** (успешная аутентификация — An account was successfully logged on) или **4625** (ошибка аутентификации — An account failed to log on). Обратите внимание на значение LogonType в событии. При входе через терминальную службу RDP — **LogonType = 10**. Если **LogonType = 7**, значит выполнено переподключение к уже имеющейся RDP сессии.



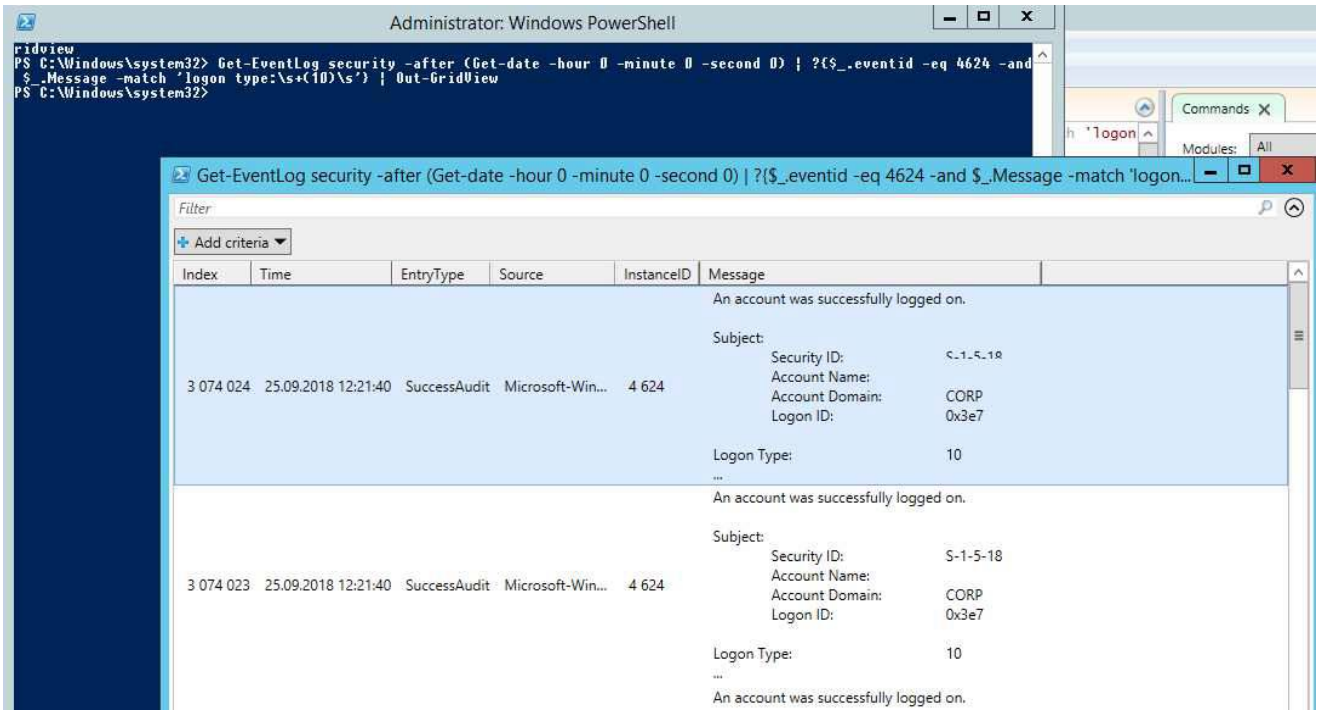
При этом имя пользователя содержится в описании события в поле **Account Name**, имя компьютера в **Workstation Name**, а имя пользователя в **Source Network Address**.

Обратите внимание на значение поля **TargetLogonID** – это уникальный идентификатор сессии пользователя с помощью которого можно отслеживать дальнейшую активность данного пользователя. Однако при отключении

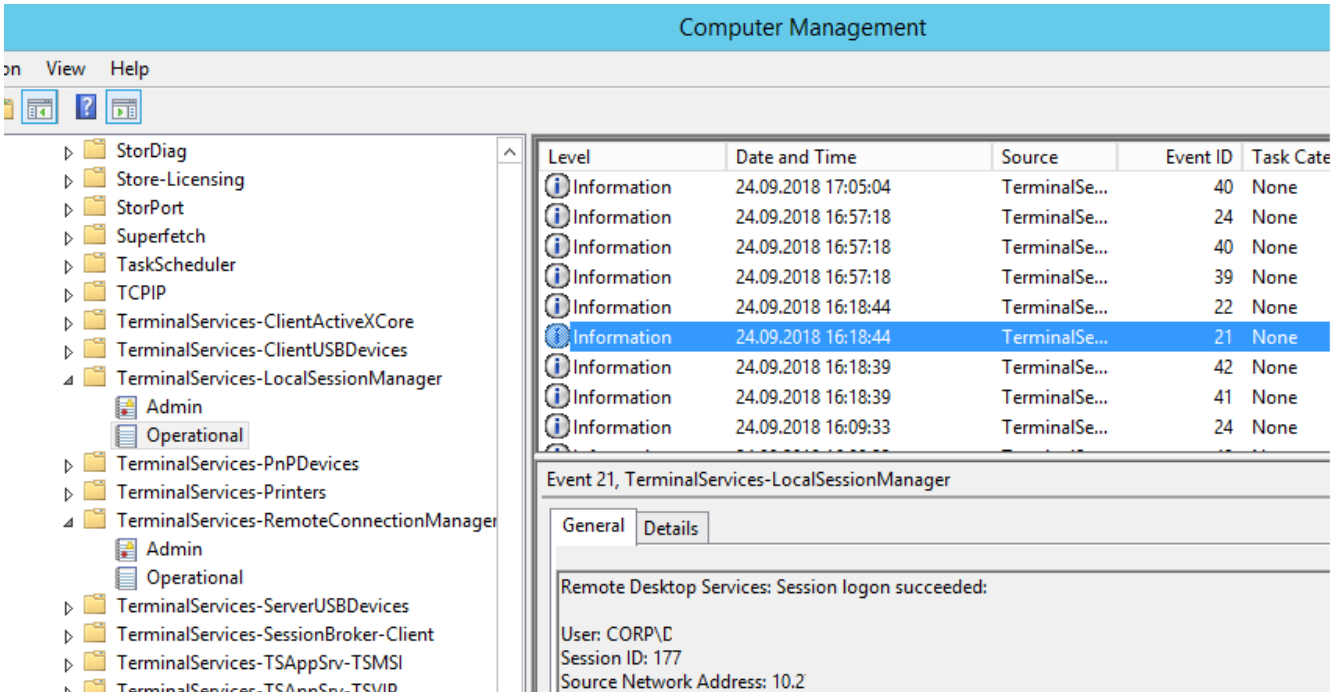
от RDP сессии (disconnect) и повторного переподключения в сессию, пользователю будет выдан новый TargetLogonID (хотя RDP сессия осталась той же самой).

Вы можете получить список событий успешных авторизаций по RDP (событие **с EventID – 4624**) с помощью такой команды PowerShell.

```
Get-EventLog security -after (Get-date -hour 0 -minute 0 -second 0) | ?{$_.eventid -eq 4624 -and $_.Message -match 'logon type:\s+(10)\s'} | Out-GridView
```



3. **Logon:** – RDP вход в систему, событие появляющееся после успешной аутентификации пользователя. Событие **с EventID – 21** (Remote Desktop Services: Session logon succeeded). Этот журнал находится в разделе Applications and Services Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational. Как вы видите здесь можно узнать идентификатор RDP сессии для пользователя — Session ID.



Событие с EventID – **21** (Remote Desktop Services: Shell start notification received) означает успешный запуск оболочки Explorer (появление окна рабочего стола в RDP сессии).

4. **Session Disconnect/Reconnect** – события отключения / переподключения к сессии имеют разные коды в зависимости от того, что вызвало отключение пользователя (отключение по неактивности, выбор пункта Disconnect в сессии, завершение RDP сессии другим пользователем или администратором и т.д.). Эти события находятся в разделе журналов Applications and Services Logs -> Microsoft -> Windows ->

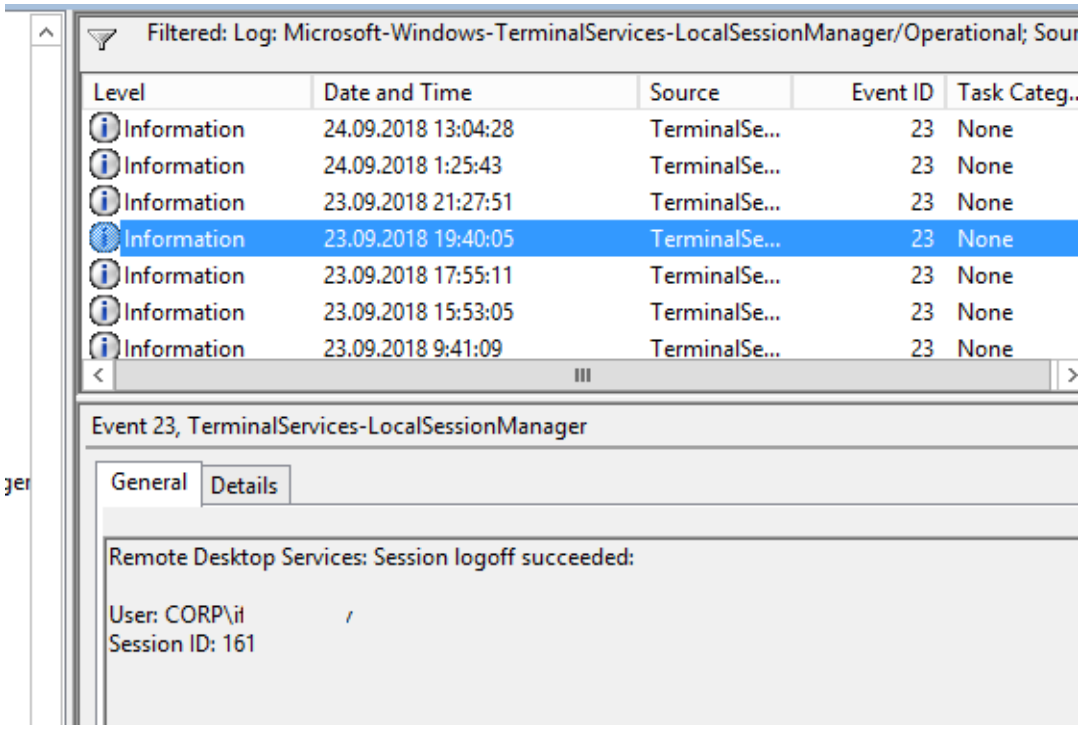
TerminalServices-LocalSessionManager -> Operational. Рассмотрим RDP события, которые могут быть интересными:

- **`EventID – 24`** (Remote Desktop Services: Session has been disconnected) – пользователь отключился от RDP сессии.
- **`EventID – 25`** (Remote Desktop Services: Session reconnection succeeded) – пользователь переподключился к своей имеющейся RDP сессии на сервере.
- **`EventID – 39`** (Session <A> has been disconnected by session <B>) – пользователь сам отключился от своей RDP сессии, выбрав соответствующий пункт меню (а не просто закрыл окно RDP клиента). Если идентификаторы сессий разные, значит пользователя отключил другой пользователь (или администратор).
- **`EventID – 40`** (Session <A> has been disconnected, reason code <B>). Здесь нужно смотреть на код причины отключения в событии. Например:
  - **reason code 0** (No additional information is available)– обычно говорит о том, что пользователь просто закрыл окно RDP клиента.
  - **reason code 5** (The client's connection was replaced by another connection) – пользователь переподключился к своей старой сессии.
  - **reason code 11** (User activity has initiated the disconnect) – пользователь сам нажал на кнопку Disconnect в меню.

Событие с EventID – **4778** в журнале Windows -> Security (A session was reconnected to a Window Station). Пользователь переподключился к RDP сессии (пользователю выдается новый LogonID).

Событие с EventID **4799** в журнале Windows -> Security (A session was disconnected from a Window Station). Отключение от RDP сеанса.

5. **Logoff:** – выход пользователя из системы. При этом в журнале Applications and Services Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational фиксируется событие с EventID **23** (Remote Desktop Services: Session logoff succeeded).

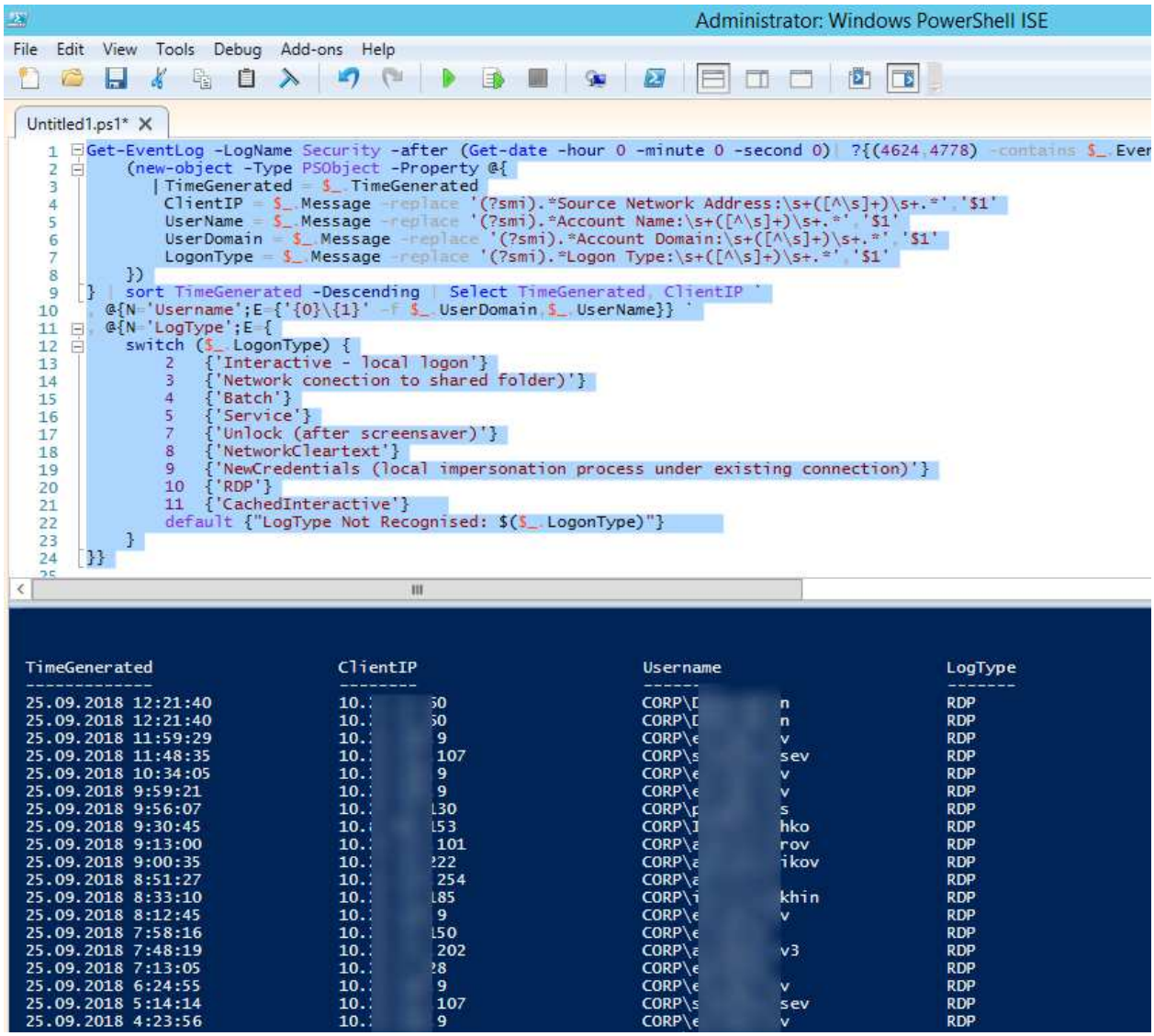


При этом в журнале Security нужно смотреть событие **с EventID – 4634** (An account was logged off).

Событие **с EventID – 9009** (The Desktop Window Manager has exited with code (<X>) в журнале System говорит о том, что пользователь инициировал завершение RDP сессии, и окно и графический shell пользователя был завершен.

Ниже представлен небольшой PowerShell, который выгружает из журналов терминального RDS сервера историю всех RDP подключений за текущий день. В полученной таблице указано время подключения, IP адрес клиента и имя RDP пользователя (при необходимости вы можете включить в отчет другие типы входов).

```
Get-EventLog -LogName Security -after (Get-date -hour 0 -minute 0 -second 0)| ?{(4624,4778) -contains
$_.EventID -and $_.Message -match 'logon type:\s+(10)\s'}| %{
(new-object -Type PSObject -Property @{
TimeGenerated = $_.TimeGenerated
ClientIP = $_.Message -replace '(?smi).*Source Network Address:\s+([^\s]+)\s+.*','$1'
UserName = $_.Message -replace '(?smi).*Account Name:\s+([^\s]+)\s+.*','$1'
UserDomain = $_.Message -replace '(?smi).*Account Domain:\s+([^\s]+)\s+.*','$1'
LogonType = $_.Message -replace '(?smi).*Logon Type:\s+([^\s]+)\s+.*','$1'
})
} | sort TimeGenerated -Descending | Select TimeGenerated, ClientIP `
, @{N='Username';E={'{0}\{1}' -f $_.UserDomain,$_.UserName}} `
, @{N='LogType';E={
switch ($_.LogonType) {
2 {'Interactive - local logon'}
3 {'Network conection to shared folder)'}
4 {'Batch'}
5 {'Service'}
7 {'Unlock (after screensaver)'}
8 {'NetworkCleartext'}
9 {'NewCredentials (local impersonation process under existing connection)'}
10 {'RDP'}
11 {'CachedInteractive'}
default {"LogType Not Recognised: $($_.LogonType)"}
}
}}
```



Иногда бывает удобно с логами в таблице Excel, в этом случае вы можете выгрузить любой журнал Windows в текстовый файл и импортировать в Excel. Экспорт журнала можно выполнить из консоли Event Viewer (конечно, при условии что логи не очищены) или через командную строку:

```
WEVTUtil query-events Security > c:\ps\security_log.txt
```

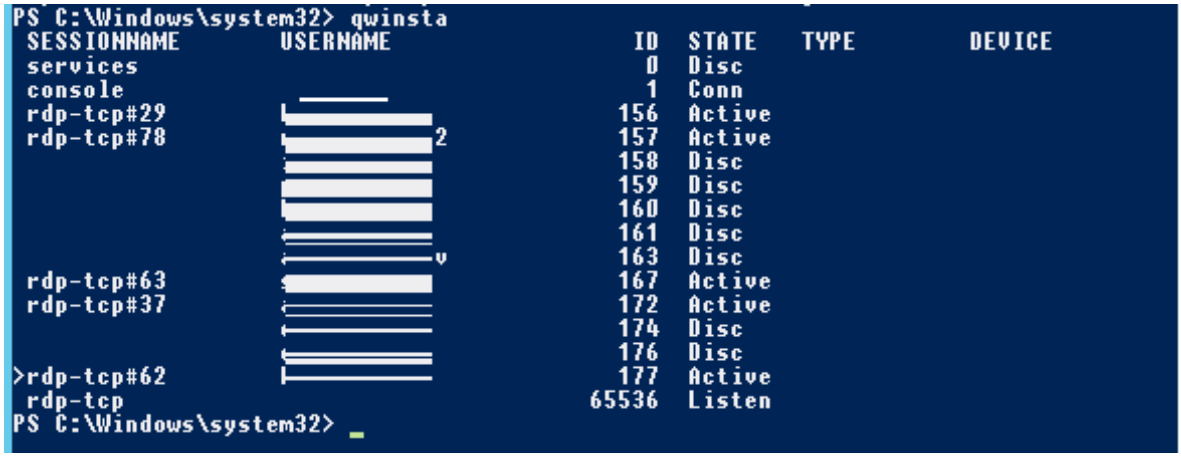
Или так:

```
get-winevent -logname "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational" | Export-Csv c:\ps\rdp-log.txt  -Encoding UTF8
```

Список текущих RDP сессий на сервере можно вывести командой:

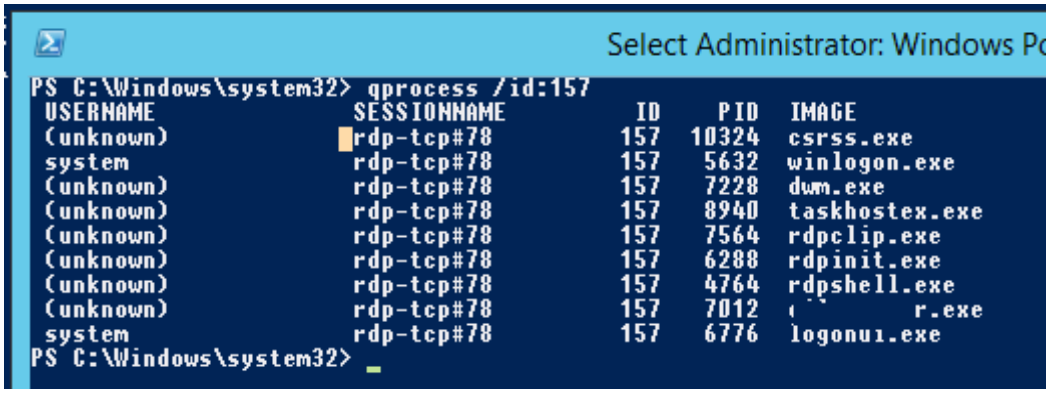
```
Qwinsta
```

Команда возвращает как идентификатор сессии (ID), имя пользователя (USERNAME)и состояние (Active/Disconnect). Эту команду удобна использовать, когда нужно определить ID RDP сессии пользователя при теневом подключении.



Список запущенных процессов в конкретной RDP сессии (указывается ID сессии):

```
qprocess /id:157
```



На RDP-клиенте логи не такие информационные, основное чем часто пользуются информация об истории RDP подключений в реестре.