SAP ГЛАЗАМИ ЗЛОУМЫШЛЕННИКА

Юдин Алексей

Positive Technologies

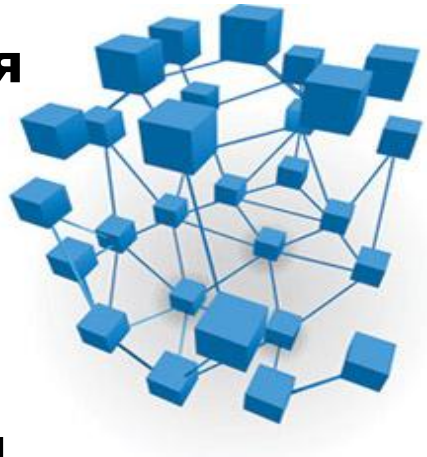
POSITIVE TECHNOLOGIES

Цели злоумышленника

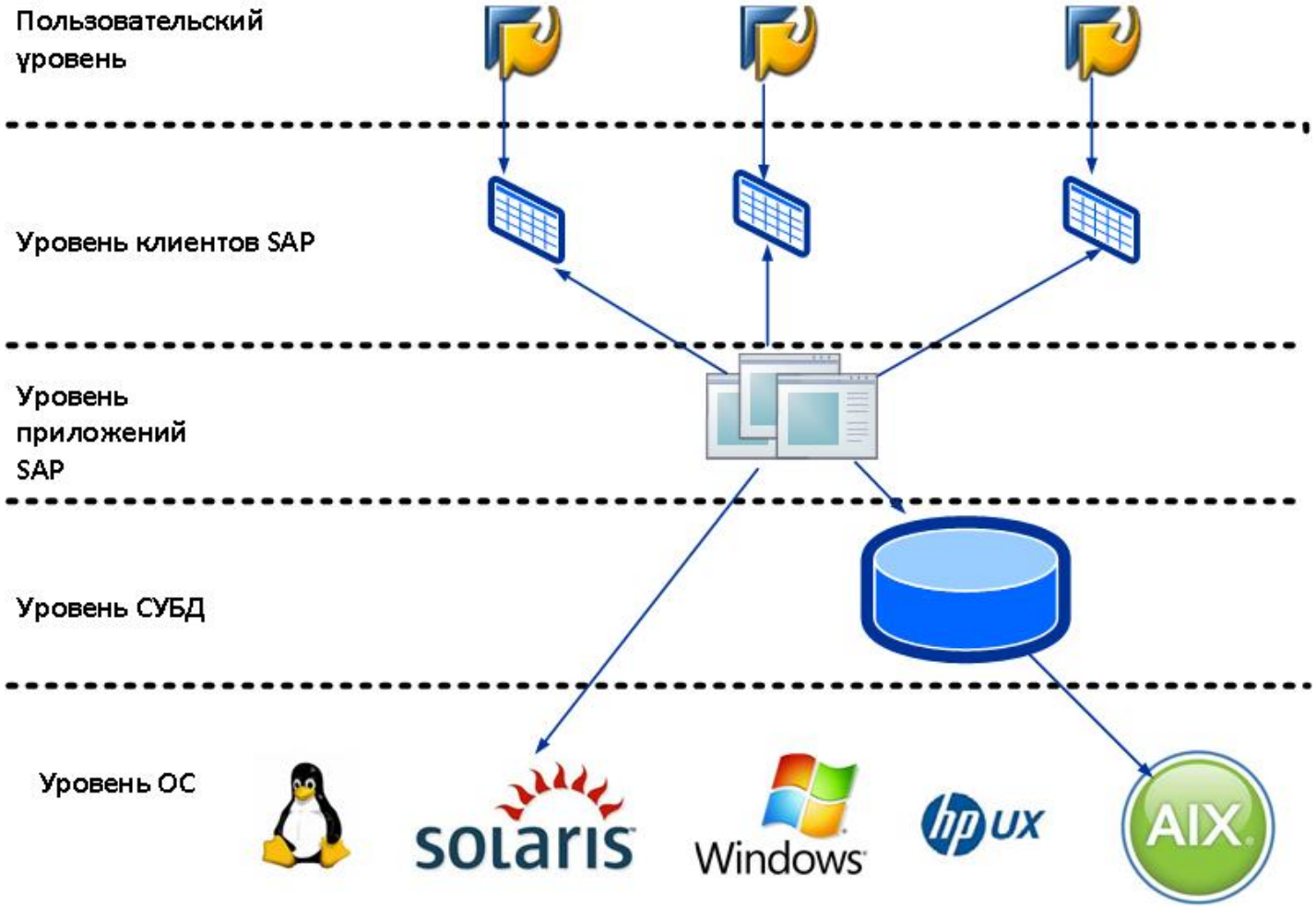
- **Получение информации**
- **Получение финансовой выгоды**
- **Нарушение работоспособности системы (бизнес функционала)**
- **Формирование плацдарма для дальнейших атак**

Особенности архитектуры SAP

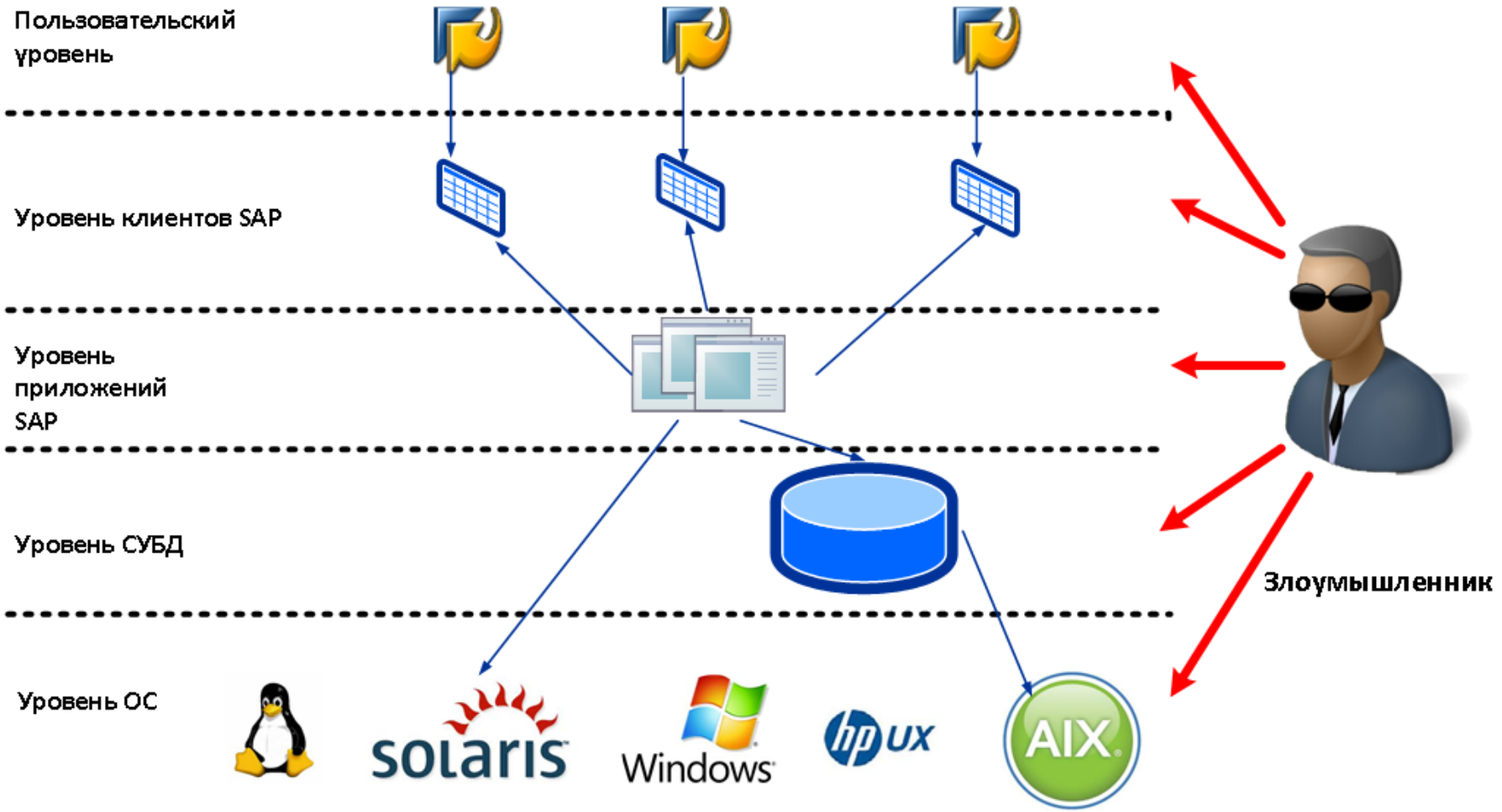
- **Различные технологические платформы, СУБД, серверы приложений,клиентское ПО**
- **Большое количество связей между компонентами**
- **Разные протоколы взаимодействия**
- **Большие объемы данных**
- **Распределенная архитектура**
- **Множество технологий разработки**



Стандартная система SAP



Направления атаки



Основной сценарий атаки

Получение доступа

- **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 систмы**

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

DEMO 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 (ОС аутентификация) получает доступ к СУБД и забирает информацию об учетной записи для последующего соединения**

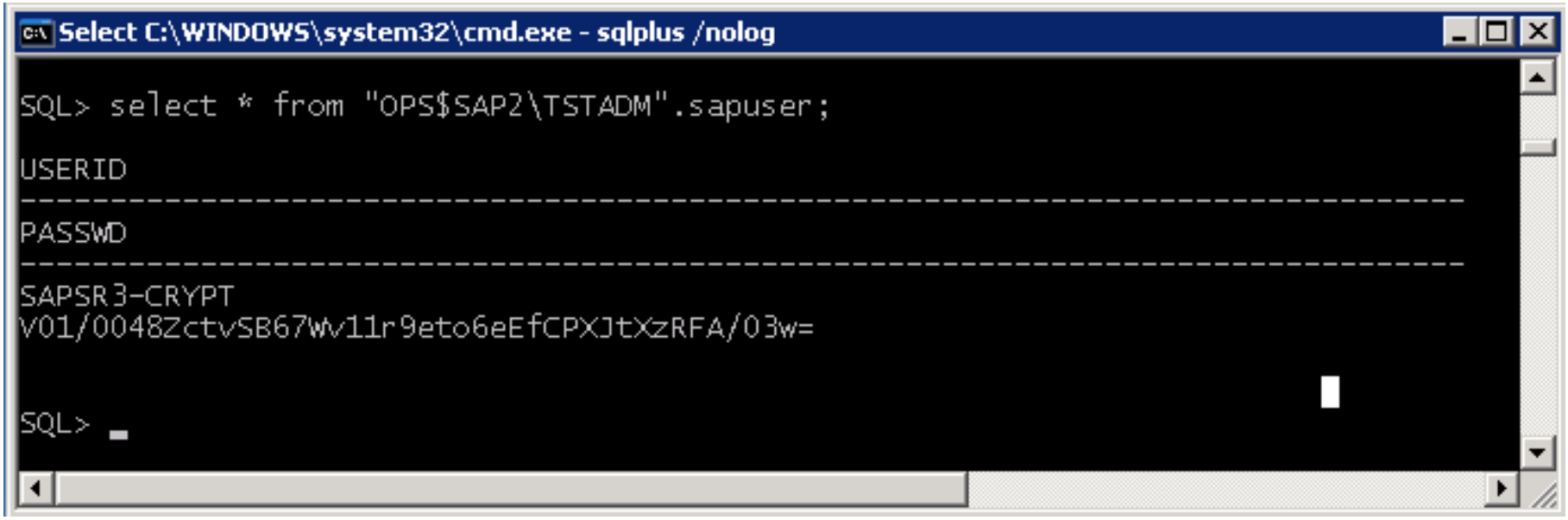
Защита аутентификационных данных

- **Данные о паролях SAPSR3 и SAPSR3DB могут хранится в открытом и шифрованном виде**
- **Шифрование – модифицированный DES с ключом ‘BE HAPPY’ зашитым в код ядра системы**
- **Пользователь OPS$<SID>ADM обладает правами SYSDBA**
- **По требованиям SAP на СУБД Oracle включен режим REMOTE_OS_AUTHENT = TRUE**
  OS_AUTHENT_PREFIX = OPS$

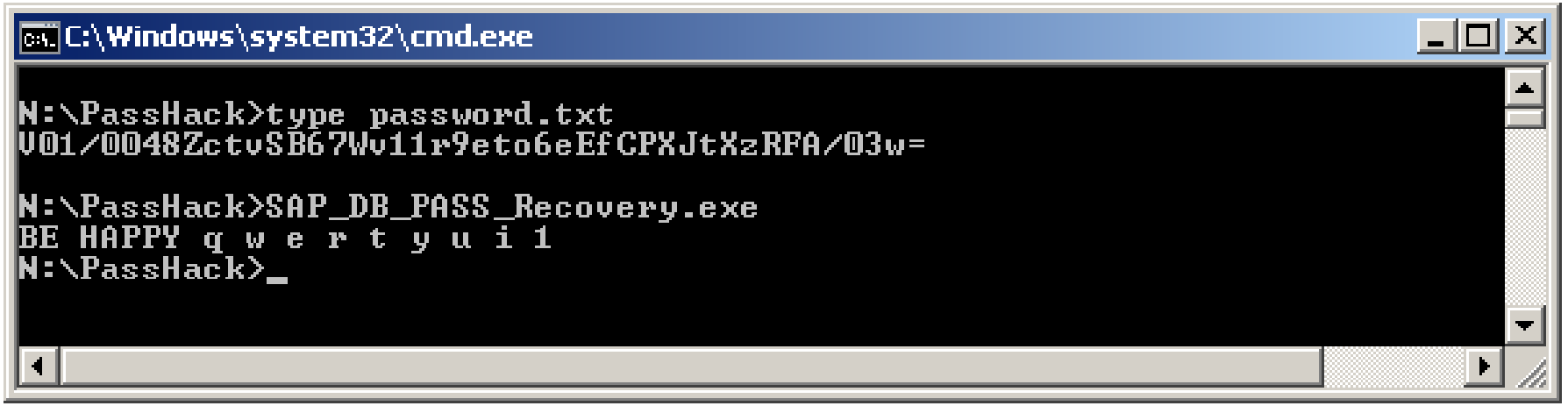
Использование Remote_OS_Authentication

- **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!**

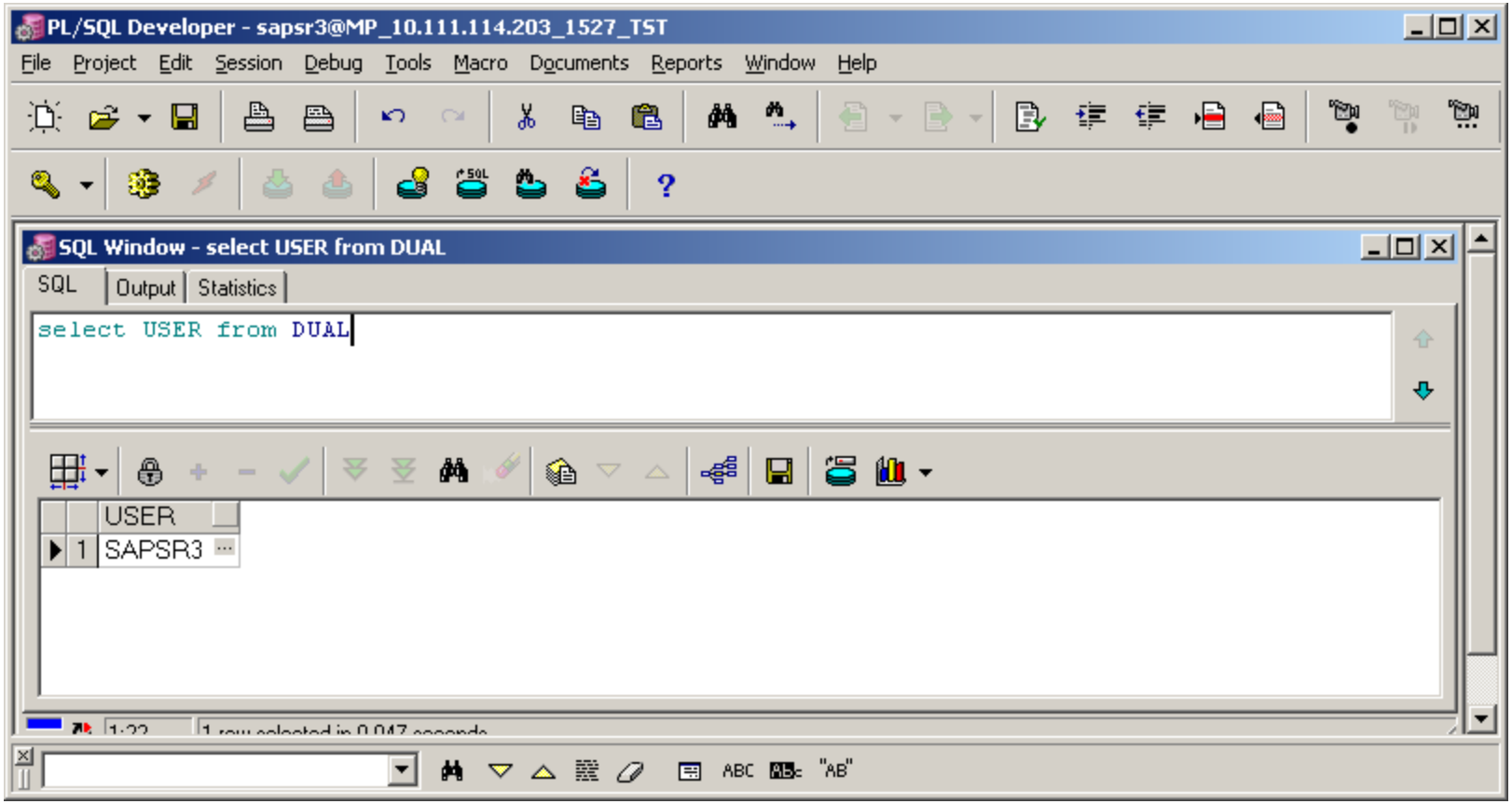
Получаем зашифрованный пароль



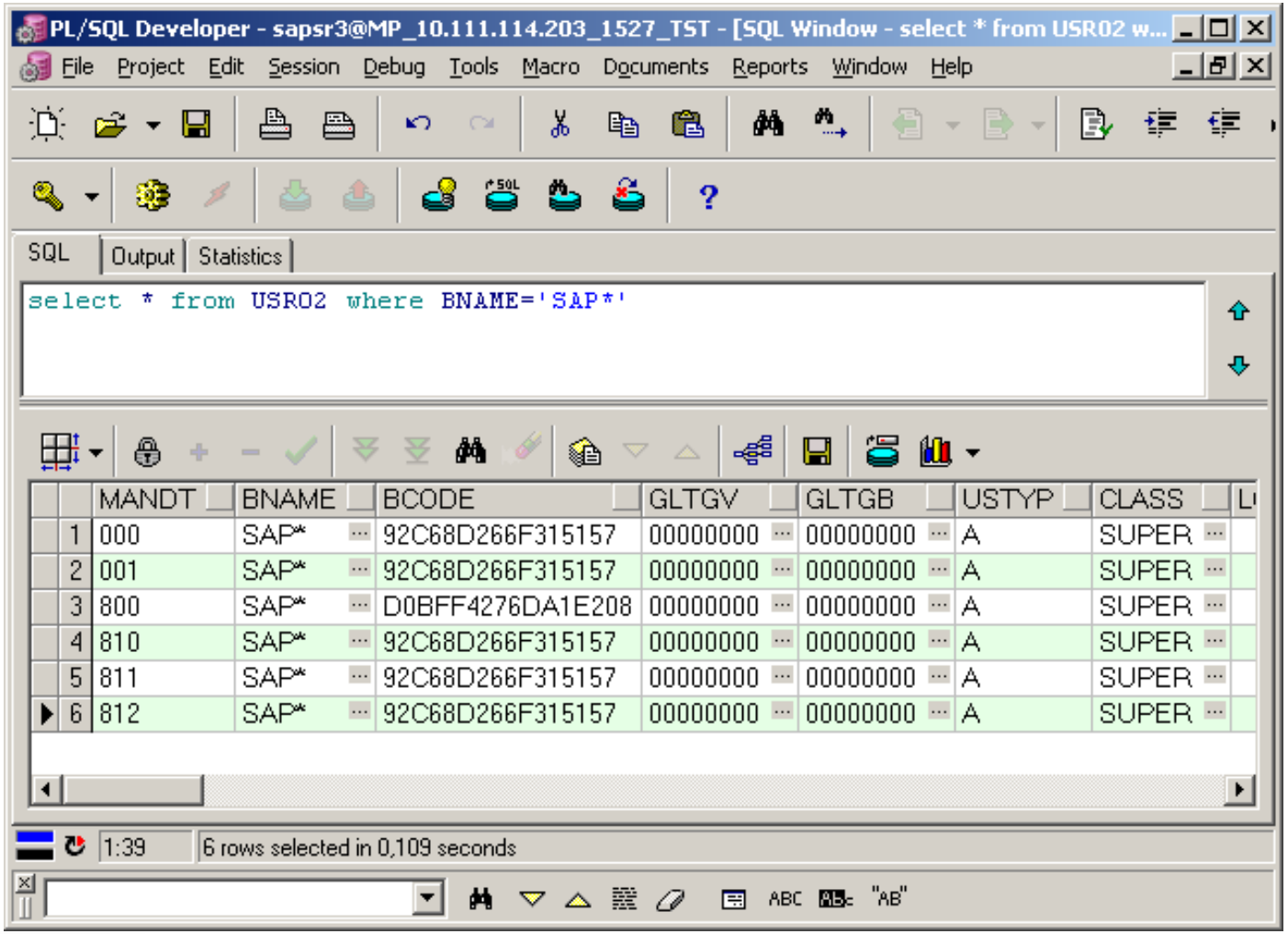
Восстанавливаем пароль



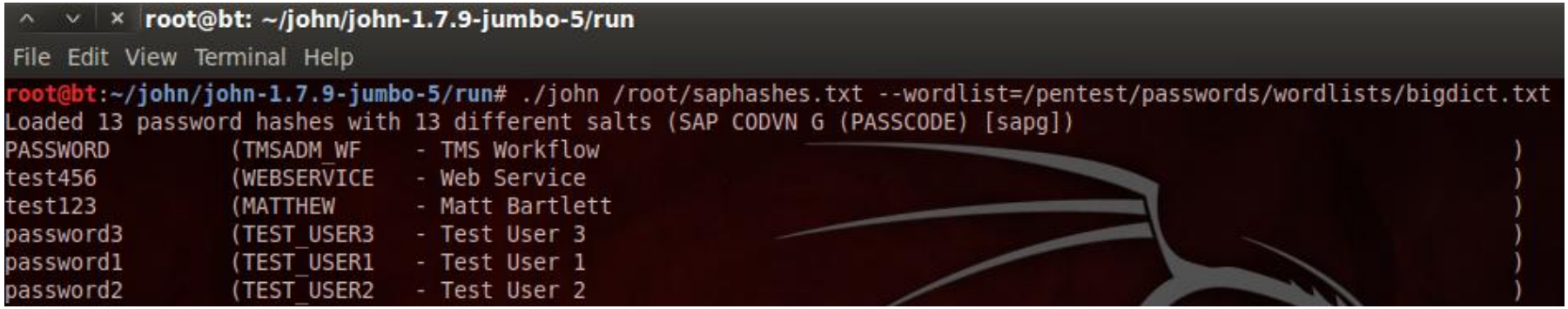
Подключаемся к БД



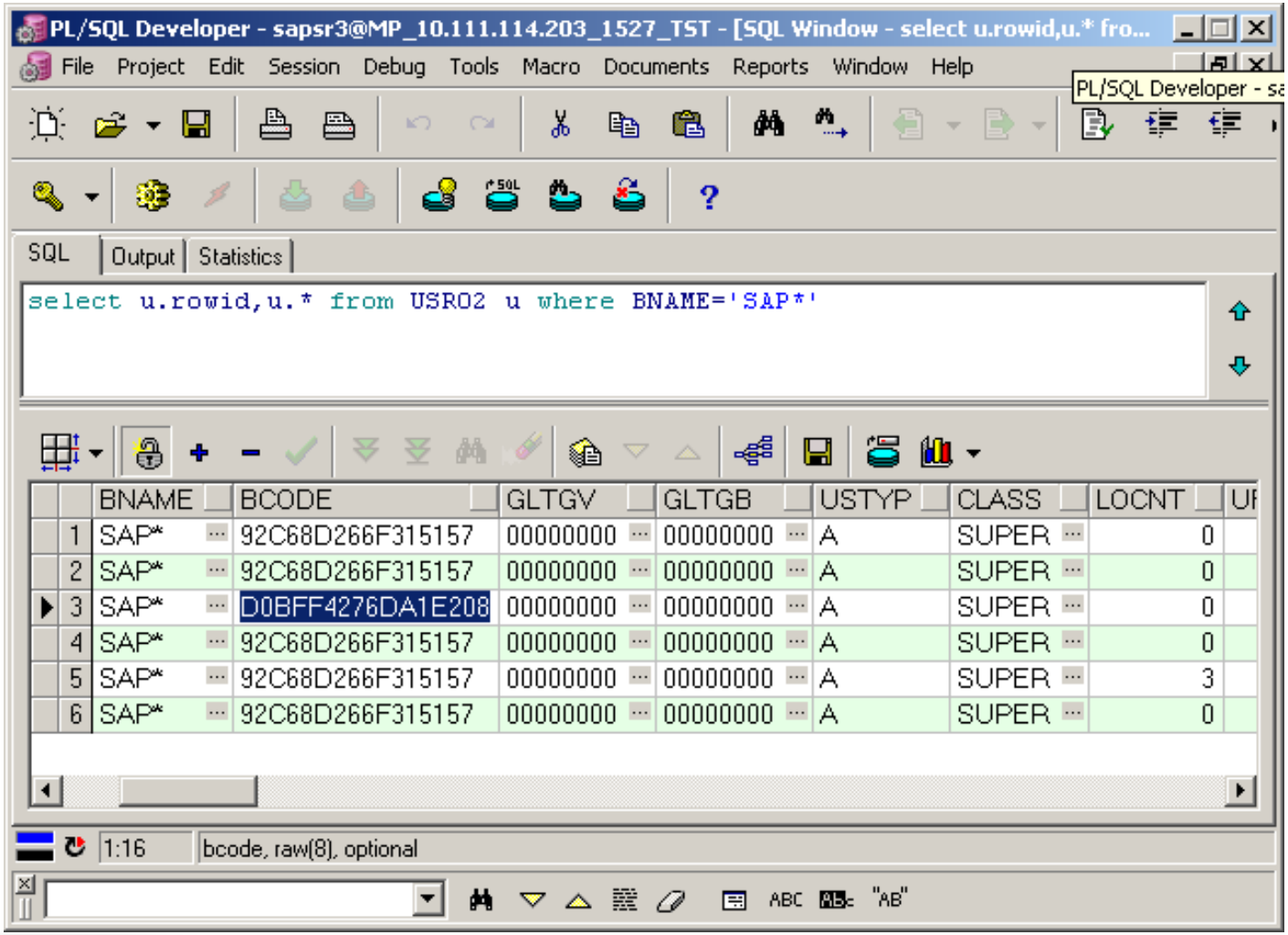
Собираем хеши пользователей



Используем John the Ripper - jumbo



Меняем хеш действующего пользователя

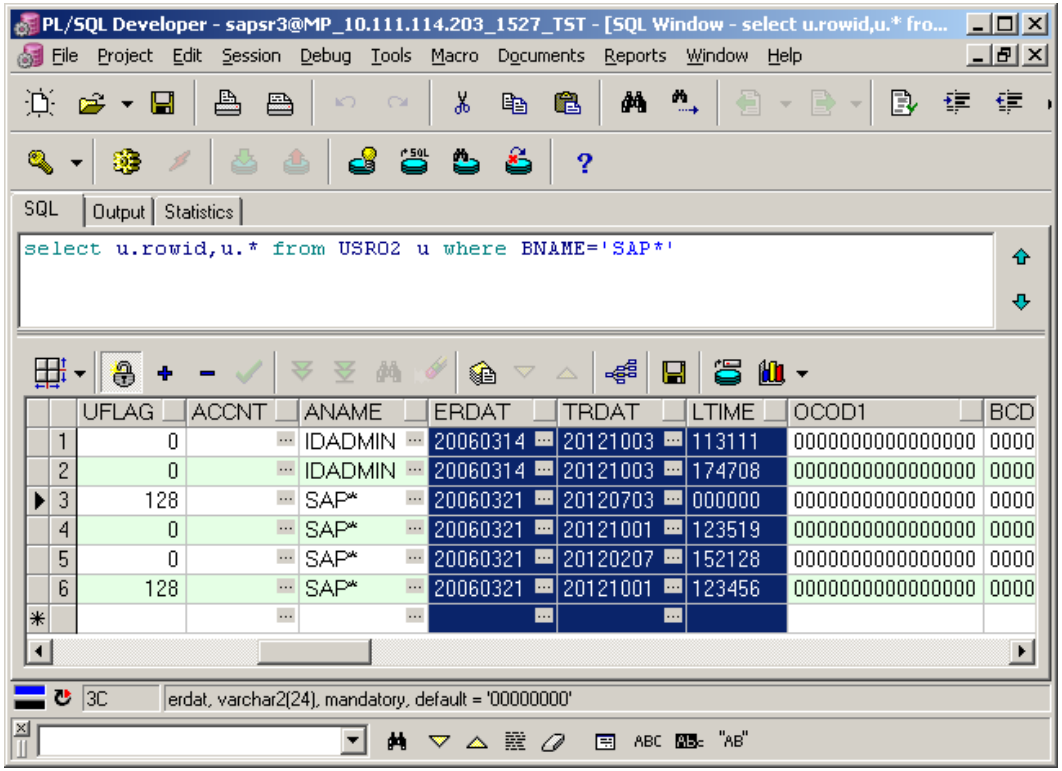


Особенности

- **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**



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

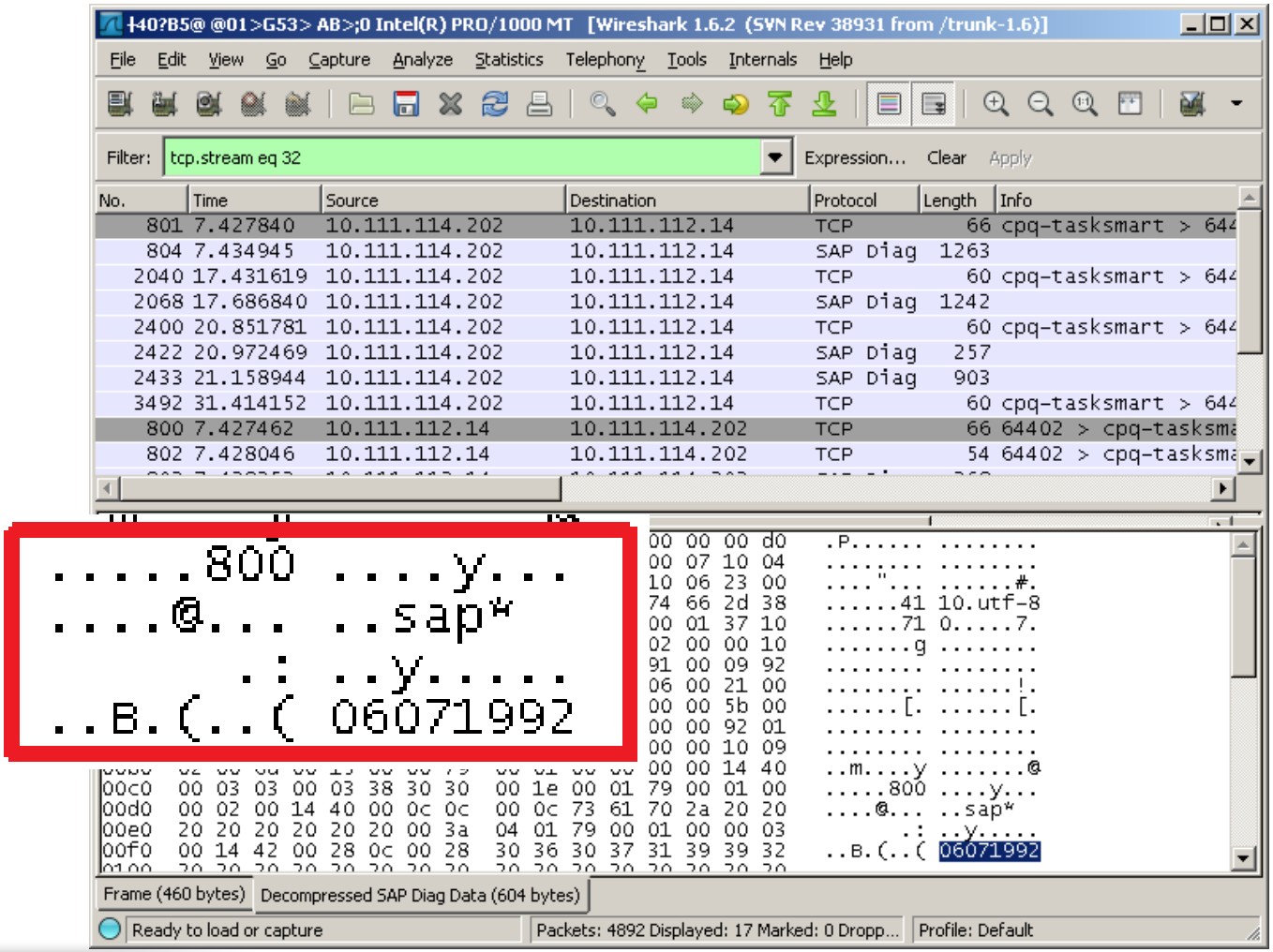
Сценарий

- 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

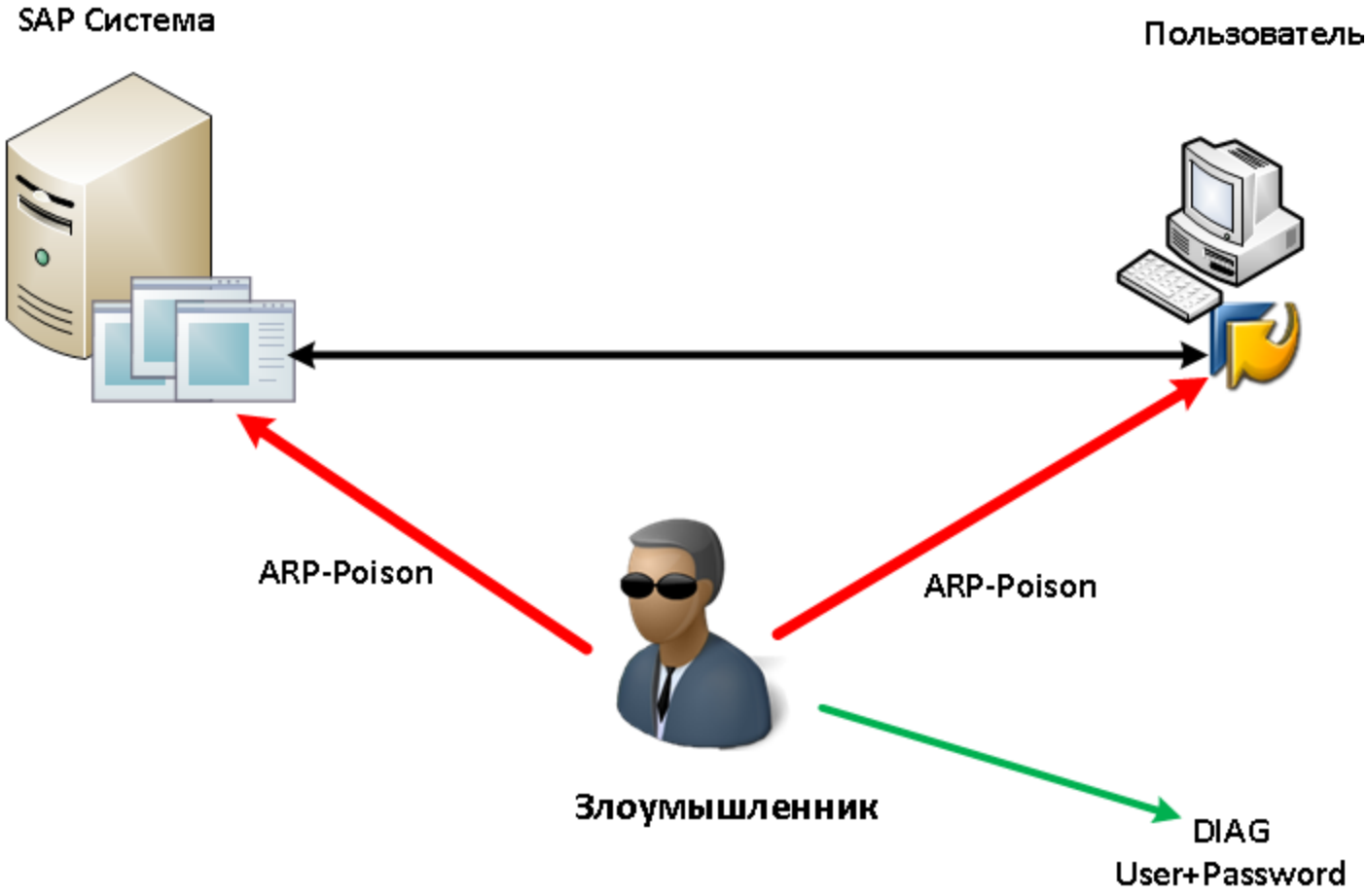
Перехват паролей

- **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)

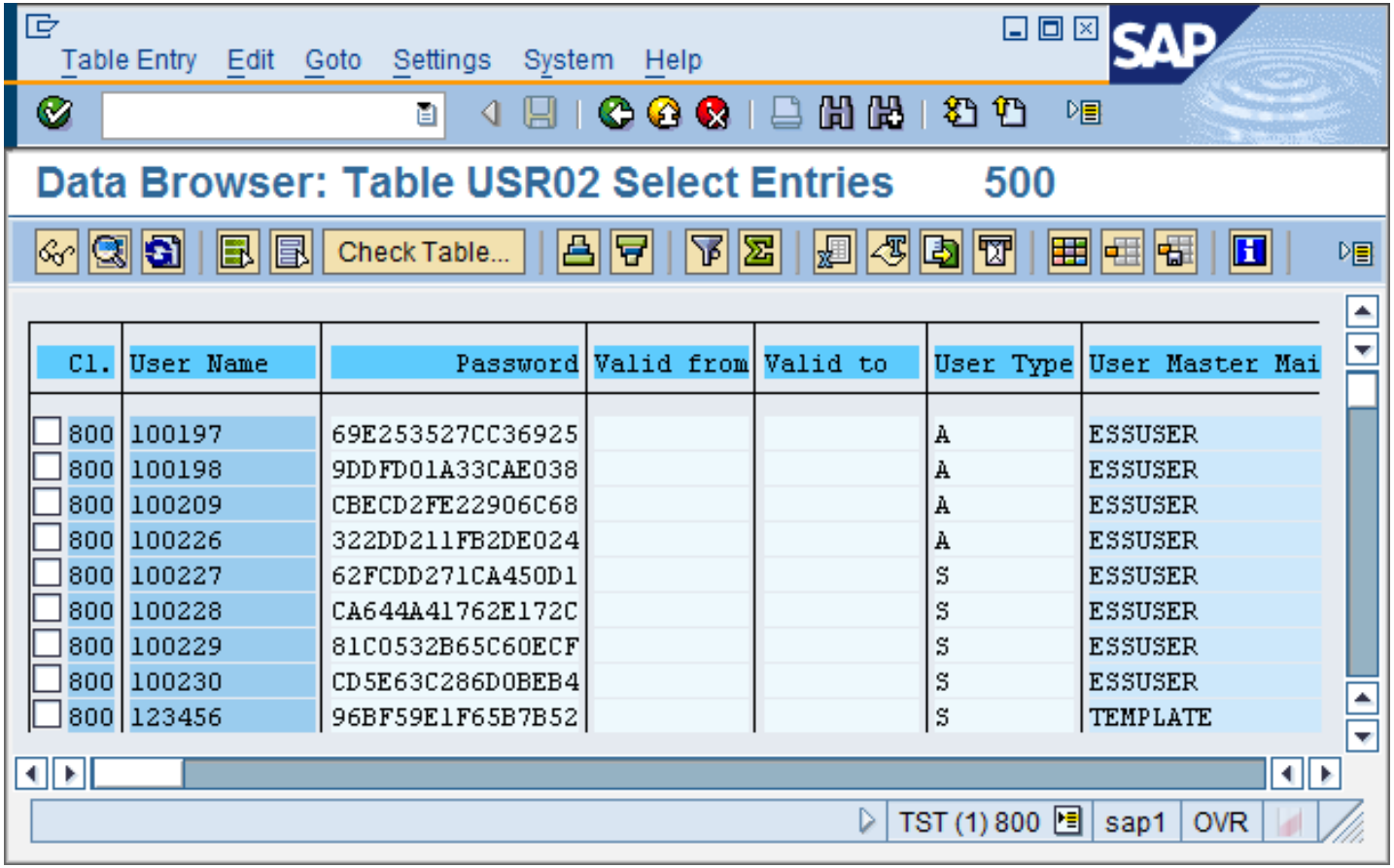
Перехват паролей DIAG



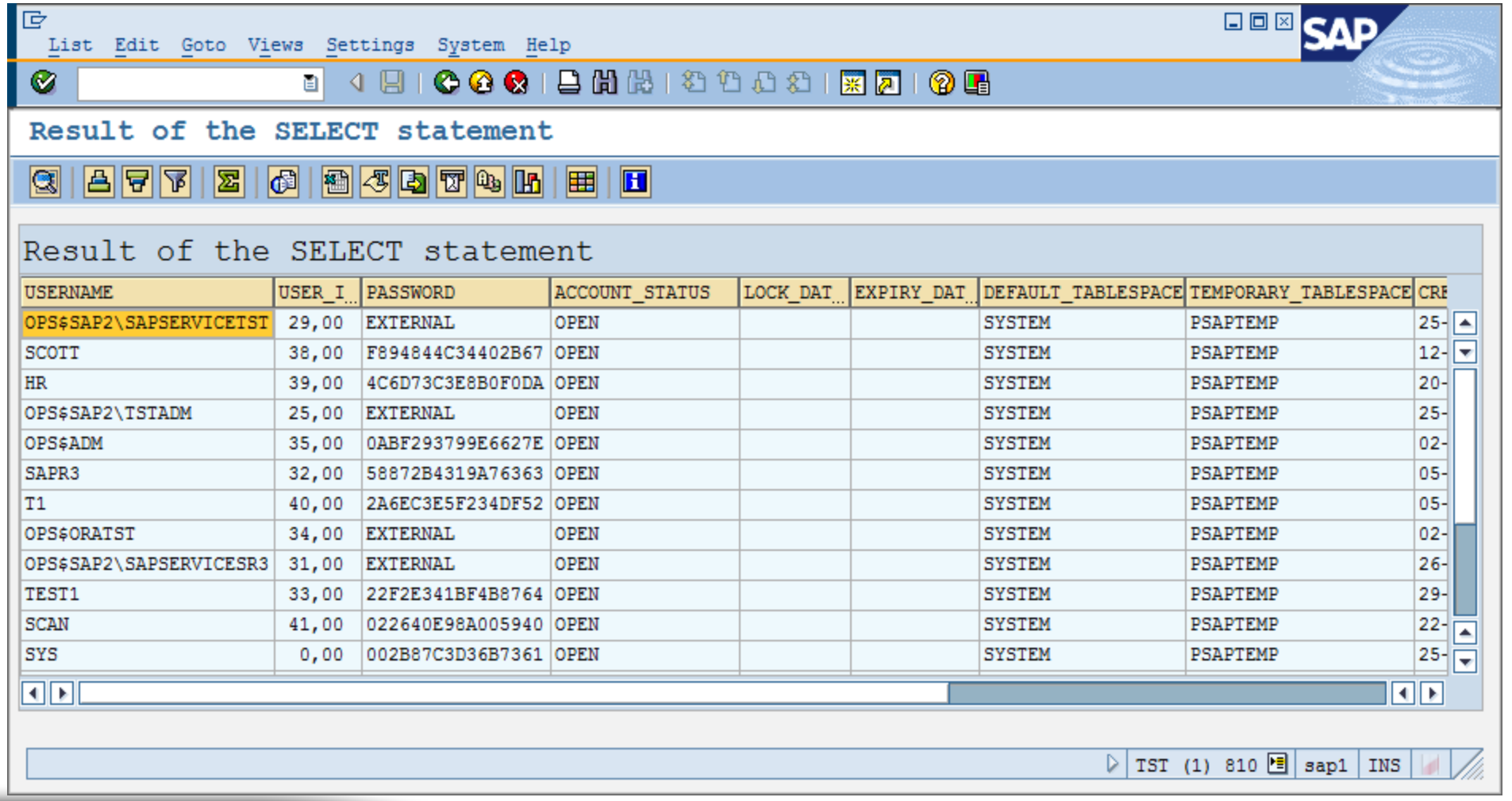
MITM


SAP Система
Пользователь
ARP-Poison
ARP-Poison
Злоумышленник
DIAG
User+Password

Получаем таблицу с хешами

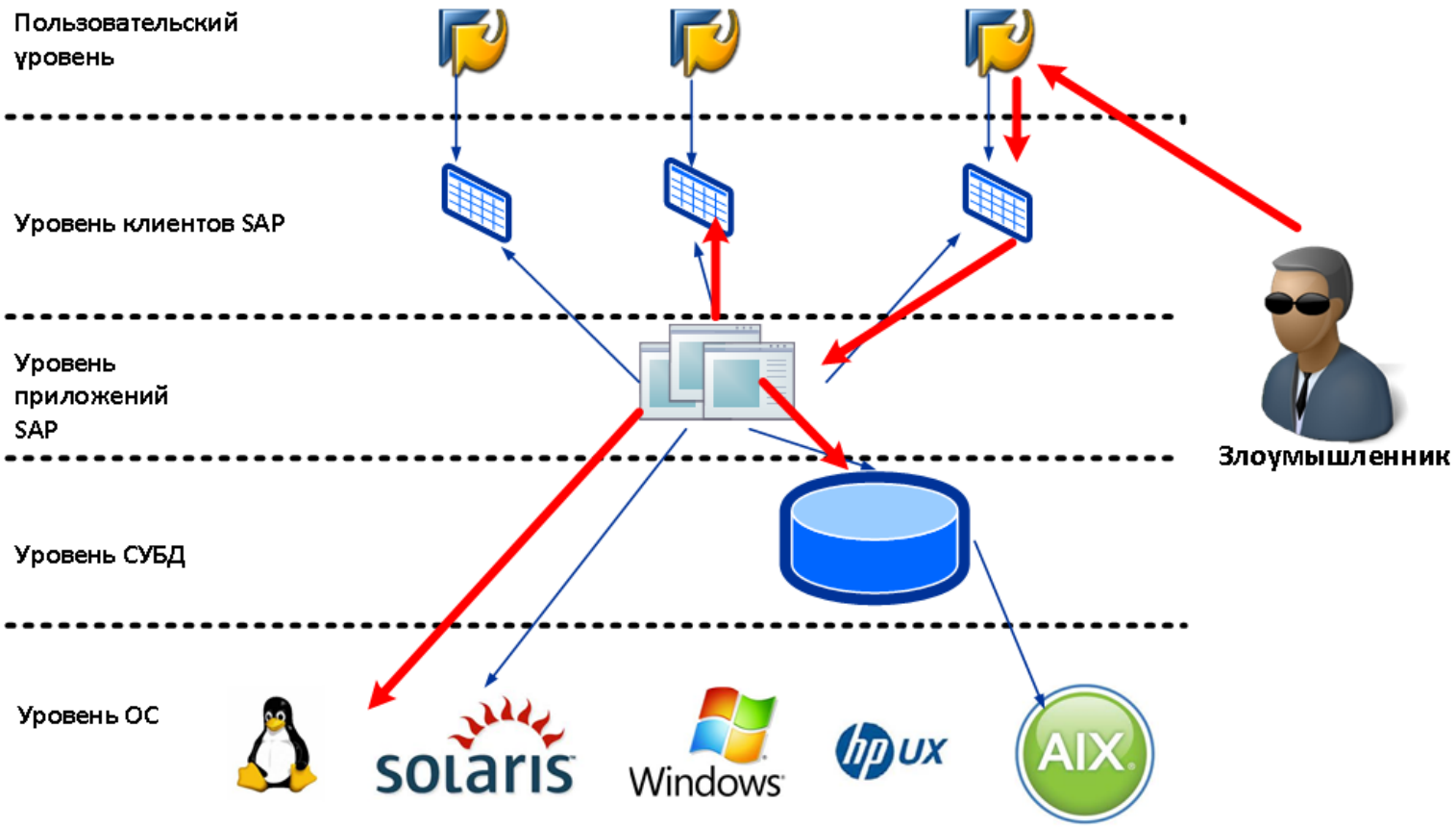


Обходим механизмы авторизации SA38->RSORADJV

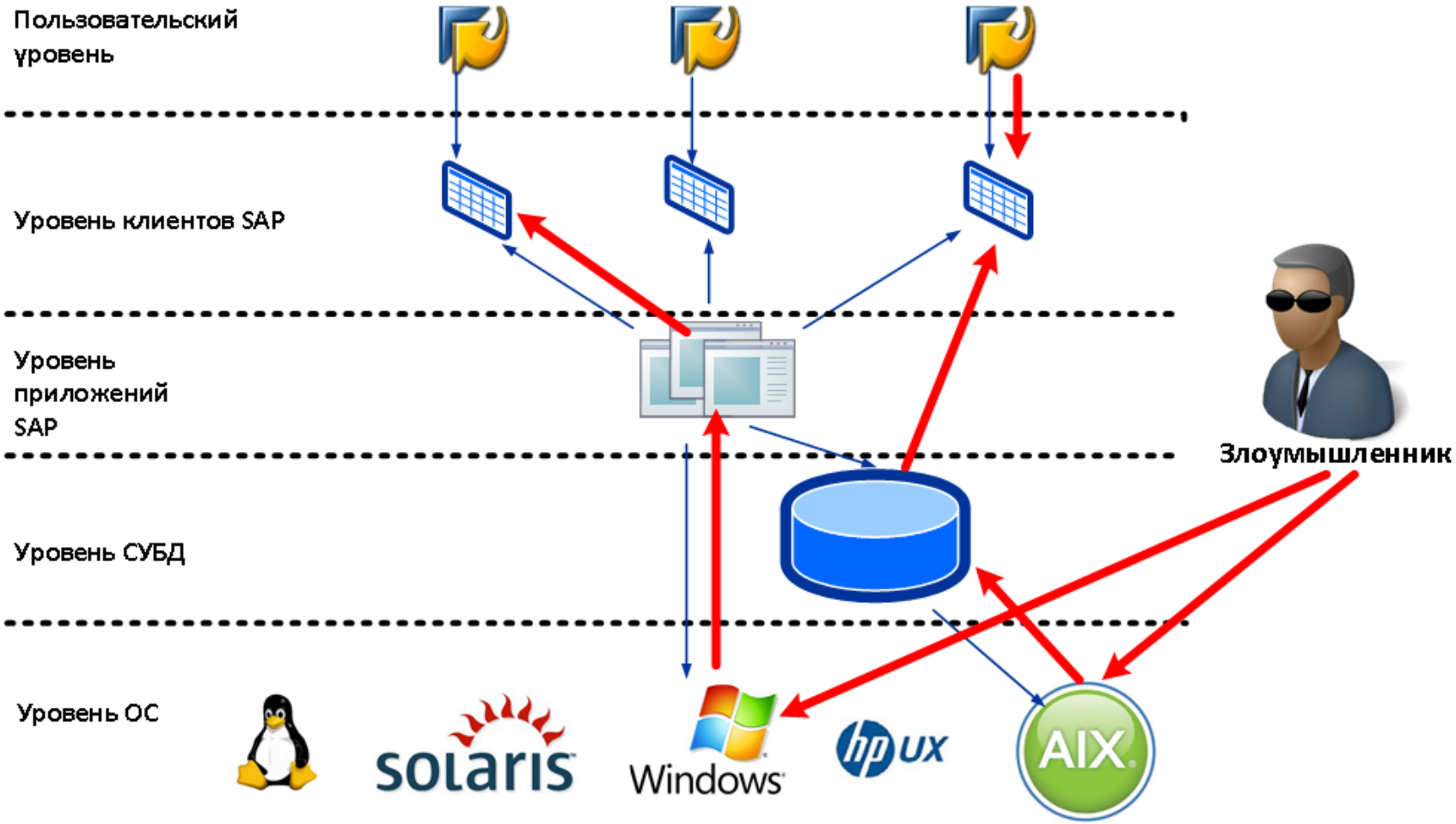


USERNAME	USER_I...	PASSWORD	ACCOUNT_STATUS	LOCK_DAT...	EXPIRY_DAT...	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE	CRE
OPS$SAP2\SAPSERVICETST	29,00	EXTERNAL	OPEN			SYSTEM	PSAPTEMP	25-
SCOTT	38,00	F894844C34402B67	OPEN			SYSTEM	PSAPTEMP	12-
HR	39,00	4C6D73C3E8B0F0DA	OPEN			SYSTEM	PSAPTEMP	20-
OPS$SAP2\TSTADM	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-

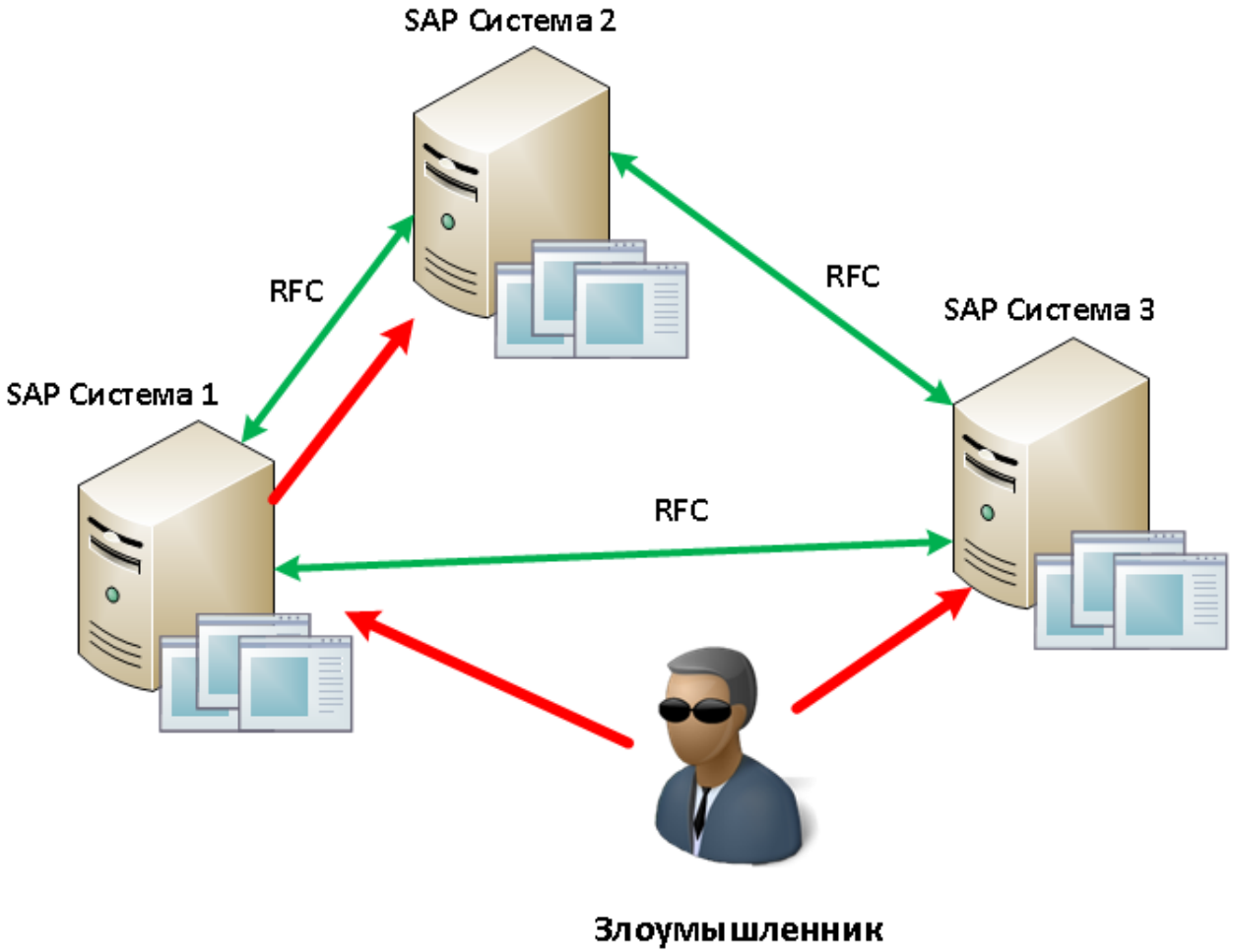
Варианты других сценариев. Атака на клиента



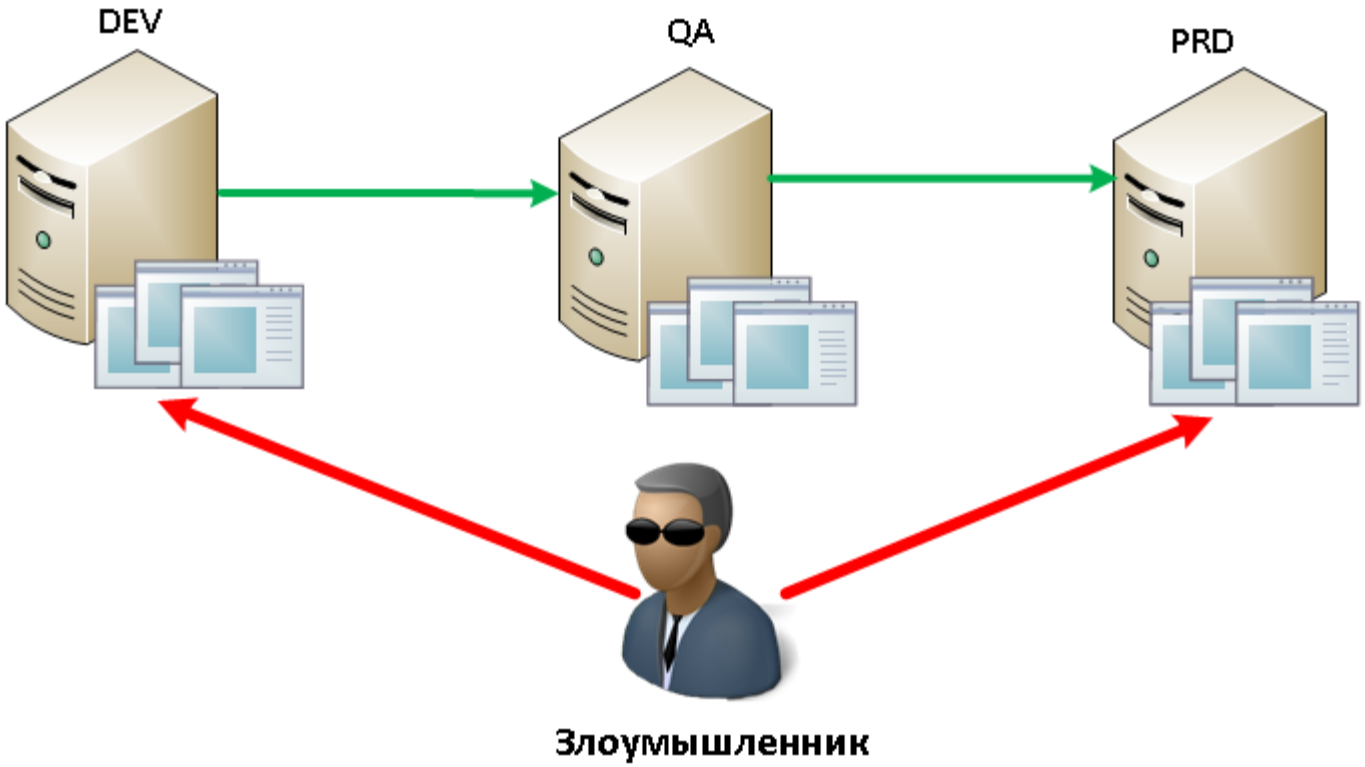
Варианты других сценариев. Атака через ОС



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

POSITIVE TECHNOLOGIES