Безопасность SAP

Аутентификация

Юдин Алексей

Positive Technologies

POSITIVE TECHNOLOGIES

Механизмы защиты

- **Обеспечение безопасности окружения (сеть, ОС, СУБД)**
- **Аутентификация**
- **Авторизация**
- **Шифрование**
- **Регистрация событий безопасности**
- **Централизованный мониторинг**
- **…**

Аутентификация в SAP системе. Основные проблемы

- Учетные записи по умолчанию
- Хранение паролей
- Инициализационные пароли
- Перехват паролей
- Подбор учетных записей и паролей
- Массовое блокирование учетных записей

Стандартные учетные записи

- **SAP* - 06071992**
- **SAP* - PASS**
- **DDIC – 19920706**
- **SAPCPIC – ADMIN**
- **EARLYWATCH - SUPPORT**
- **TMSADM – PASSWORD**

Report RSUSR003

Check the Passwords of Standard Users in All Clients

Client	User	Lock	Password Status	Reason for User Lock
000	DDIC		Exists; Password not trivial.	
	SAP*		Exists; Password not trivial.	
	SAPCPIC		Password ADMIN well known. See SAP Note 29276	User ID Is Not a System User
001	DDIC		Exists; Password not trivial.	
	SAP*		Exists; Password not trivial.	
	SAPCPIC		Password ADMIN well known. See SAP Note 29276	User ID Is Not a System User
066	DDIC		Exists; Password not trivial.	
	EARLYWATCH		Does not exist.	
	SAP*		Exists; Password not trivial.	
	SAPCPIC		Does not exist.	
800	DDIC		Exists; Password not trivial.	
	SAP*		Password 06071992 well known.	
	SAPCPIC		Password ADMIN well known. See SAP Note 29276	User ID Is Not a System User

SAP*

- **Создать учетную запись во всех мандантах**
- **Заблокировать SAP***
- **Ограничить права (убрать SAP_ALL)**
- **Использовать настройки профиля *"login/no_automatic_user-sapstar=1"***

SAPCPIC

- **Права администратора по умолчанию**
- **Возможность получить таблицу USR02 с хешами паролей пользователей**
- **Практически не блокируется в системах**
- **Доступное программное обеспечение для работы с RFC**
  - http://rfcconnector.com/documentation/examples/excel/
  - http://download.cnet.com/MIL-Read-Table/3000-10254_4-10767704.html
  - …

Хранение паролей

- **Пароли ABAP пользователей хранятся в таблицах USR02, USH02, USRPWDHISTORY**
- **Различные алгоритмы хеширования: A,B,D,E,F,G,H,I**
- **Наличие уязвимостей в алгоритмах хеширования**
- **Автоматизированные средства анализа стойкости паролей**
  - **JohnTheRipper + SAP Patch (A,B,G)**
  - **SAPHash Positive Research Lab**
  - **MaxPatrol**

Уязвимости алгоритмов хеширования

- **CODVN A – устаревший алгоритм разработанный SAP – длина пароля <=8, символы в UPPERCASE**
- **CODVN B – устаревший алгоритм на базе MD5, длина пароля <=8 остальная часть пароля обрезается, все символы в UPPERCASE, спецсимволы заменяются на символ ^**

	BNAME	BCODE	CODVN	PASSCODE	PWDSALTEDHASH
☐	ABELT	996B971C3BCAA39C	B	000000000000000000000000000000000000000000	

BNAME	BCODE
SAP*	D0BFF4276DA1E208

Уязвимости алгоритмов хеширования

- **CODVN D – также устаревший алгоритм предназначался для того чтобы исправить ошибки алгоритма B – в части урезания паролей и использования спец символов**

- **CODVN E – пришел на смену паролям B и D и был призван устранить их проблемы, работает в версиях с 4.6x до 6.x**
  - **SAP Note 874738 - New password hash calculation procedure (code version E)**

Уязвимости алгоритмов хеширования

- **CODVN F – наиболее часто используемый на текущий момент алгоритм хеширования, основан на SHA1, длина пароля до 40 символов , перед хешированием строки переводятся в UTF-8, поэтому символы могут быть практически любые, работает в версиях начиная с 7.00**

	BNAME	PASSCODE
☐	SAP*	8948310AF768FA9061598E8F68FD144CE65B7480

Уязвимости алгоритмов хеширования

- **CODVN G = B+F – можно подобрать сначала часть пароля размером в 8 символов по алгоритму B а затем использовать эту часть для подбора пароля по алгоритму G, работает в версиях начиная с 7.00**

	BNAME	BCODE	PASSCODE
☐	SAP*	D0BFF4276DA1E208	8948310AF768FA9061598E8F68FD144CE65B7480

Уязвимости алгоритмов хеширования

- **CODVN H – наиболее безопасный алгоритм хеширования – основан на SHA1 с переменной длиной соли, работает в версиях начиная с 7.02**

- **CODVN I = B+F+H – проблемы аналогичные G**

BNAME	BCODE	PASSCODE
SAP*	D0BFF4276DA1E208	8948310AF768FA9061598E8F68FD144CE65B7480

PWDSALTEDHASH
{x-issha, 1024}k/iSzGRiAy/g7vo2gZljkul7rKkjx5TvrstNH+cn0Mg=

- **Скорость подбора паролей**
  - **до 700 000 паролей в секунду для CODVN B**
  - **до 300 000 паролей в секунду для CODVN G**

Password Compatibility

- **login/password_downwards_compatibility =**
- **0 – отключить совместимость - БЕЗОПАСНО**
- **1,2,3,4,5 – включают совместимость, хранятся все хеши паролей**
- **Отчет CLEANUP_PASSWORD_HASH_VALUES**
- **Note 1458262 - ABAP: recommended settings for password hash algorithms**

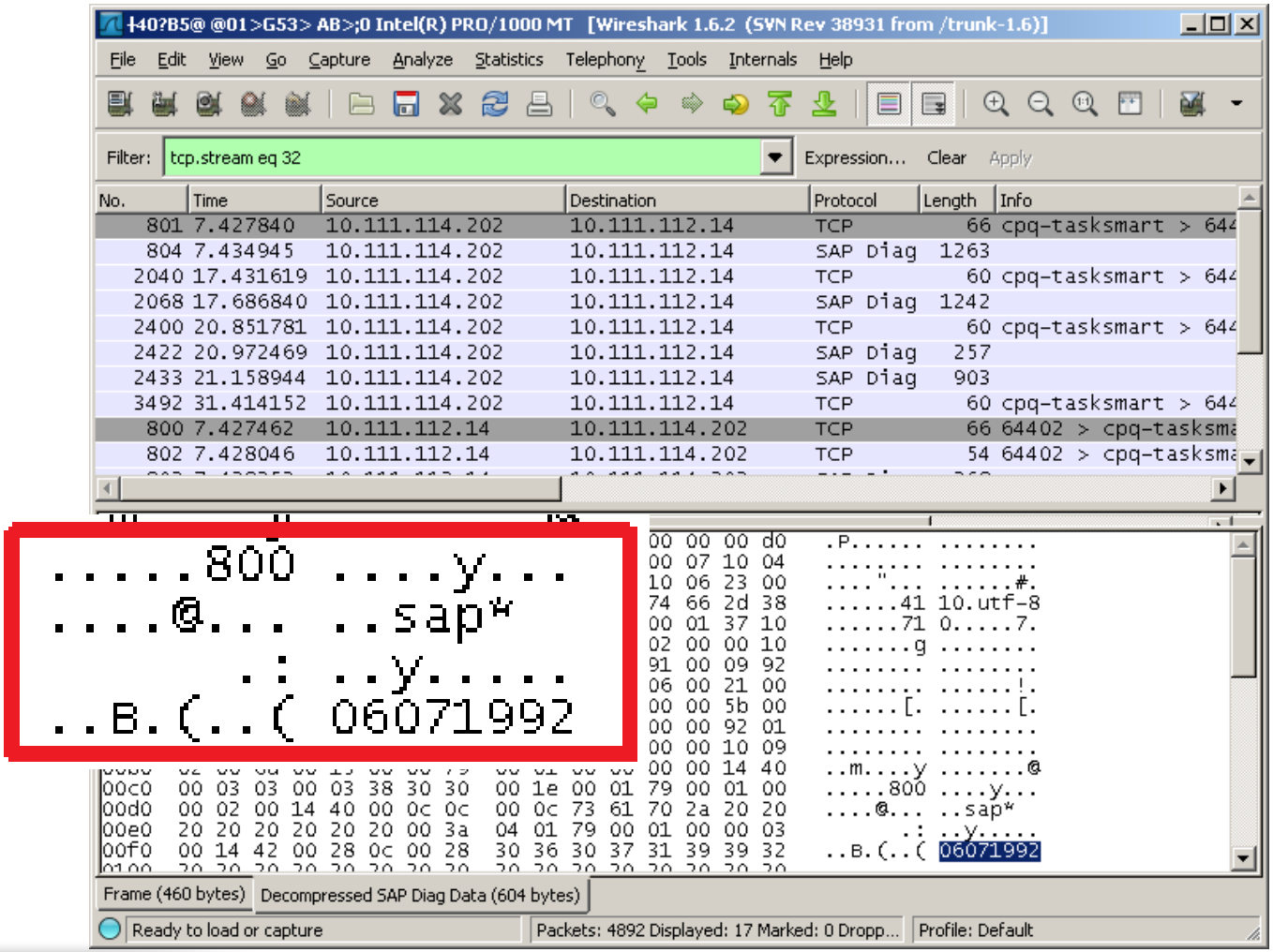
Инициализационные пароли

- **Простые инициализационные пароли: 123456, 1234567, 12345678 …**
- **Неограниченный срок действия инициализационных пароле**
  - **login/password_max_idle_initial=0 (deactivated by default)**
  - **login/password_max_idle_initial=0 (deactivated by default)**
- **Отсутствие требований по сложности для паролей устанавливаемых администратором**

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)

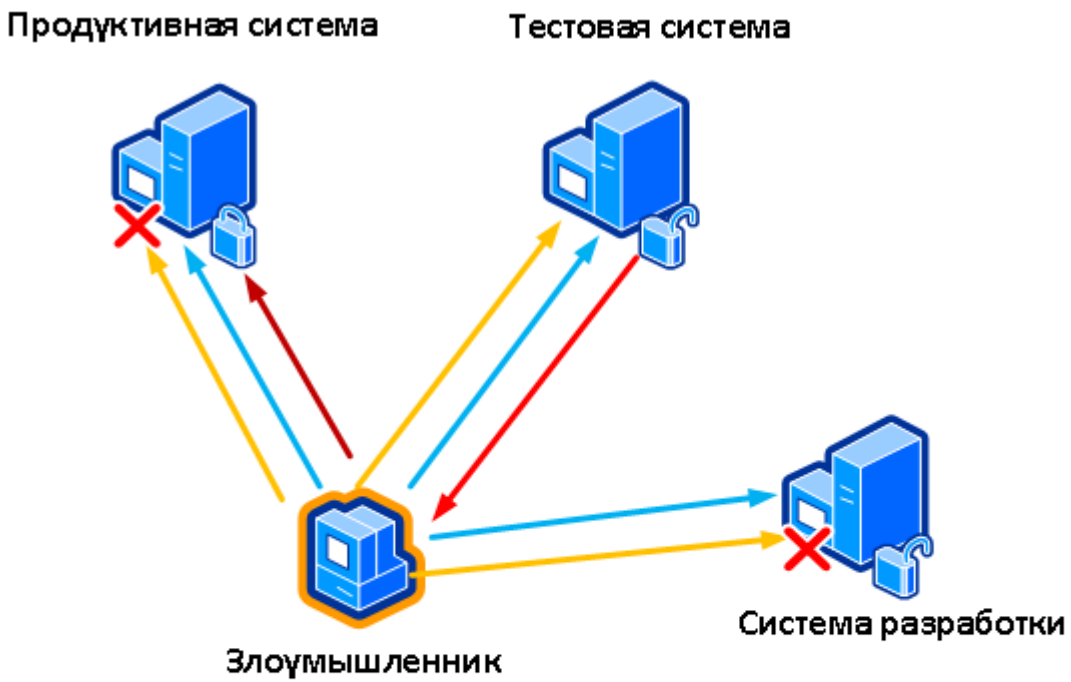
Перехват паролей DIAG



Сценарий атаки

- **Поиск SAP систем и доступных сервисов**
- **Попытка подбора паролей**
  - **Проверка стандартных учетных записей**
  - **Подбор паролей с использованием списка сотрудников компании (полученных из AD, телефонных справочников, Email…)**
- **Перехват паролей пользователей (MITM)**
- **Получение и анализ хешей паролей**
- **Попытки входа в другие SAP системы с использованием полученных учетных записей**

Схема атаки


Продуктивная система
Тестовая система
Злоумышленник
Система разработки
Сканирование информационных систем
Попытка подбора пользователей и паролей
Получение списка пользователей и подбор паролей по хешу
Попытка доступа к системе с использованием известных имен пользователей и паролей

Pentest

- **Определение SAP сервисов**
- **Поиск клиентов**
- **Подбор паролей через RFC и DIAG**
- **Проверка на отсутствие шифрования**

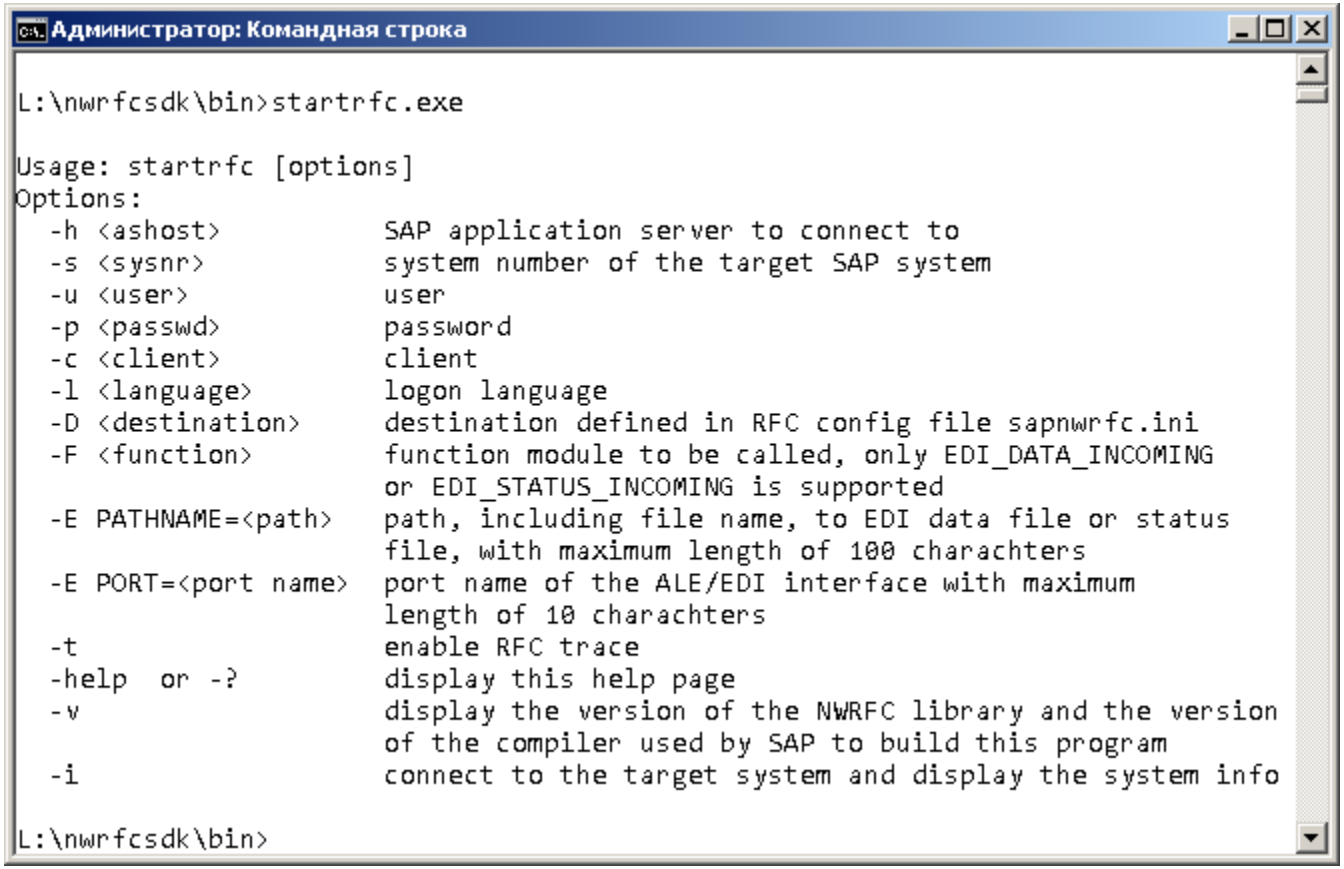
SAP TCP Ports

Service	Port Number / Service Name Rule	External	Default	Range (min-max)	Fixed
NetWeaver Application Server ABAP including Internet Conn					
Dispatcher	32NN sapdpNN	+	3200	3200-3299 sapdp00-sapdp99	+
Gateway	33NN sapgwNN	+	3300	3300-3399 sapgw00-sapgw99	+

Автоматизация атаки. SAP RFCSDK

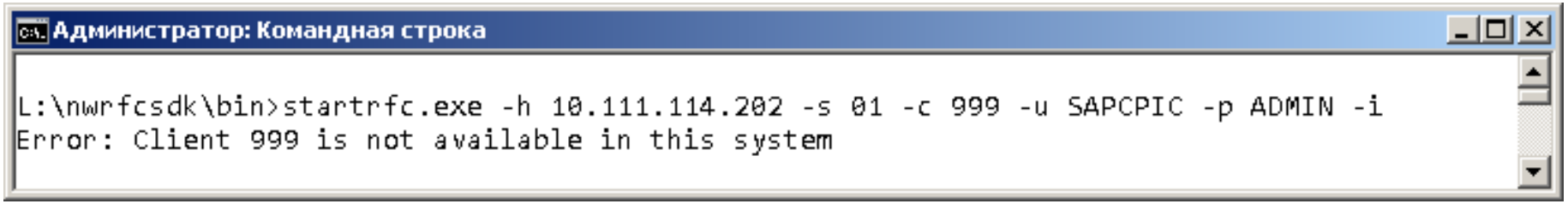
- **SAP RFCSDK – библиотека для разработки приложений работающих с SAP системой по протоколу SAP RFC**
- **Можно найти в сети Интернет**
- **Содержит утилиту для тестирования RFC - Startrfc.exe**
- **Может использоваться для интеграции с PHP, Perl, VB, C++ ….**

StartRFC.exe

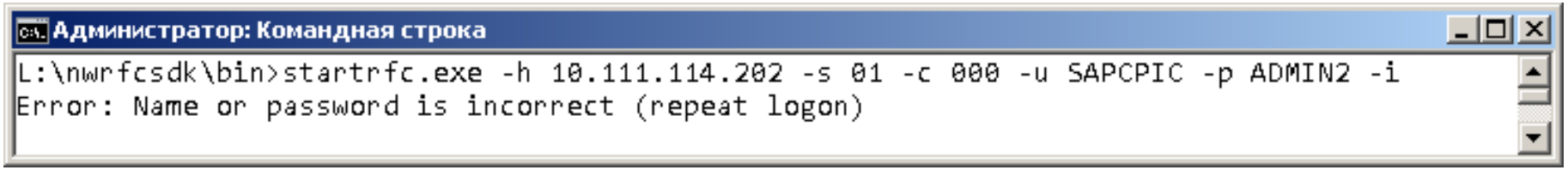


StartRFC.exe – получение информации

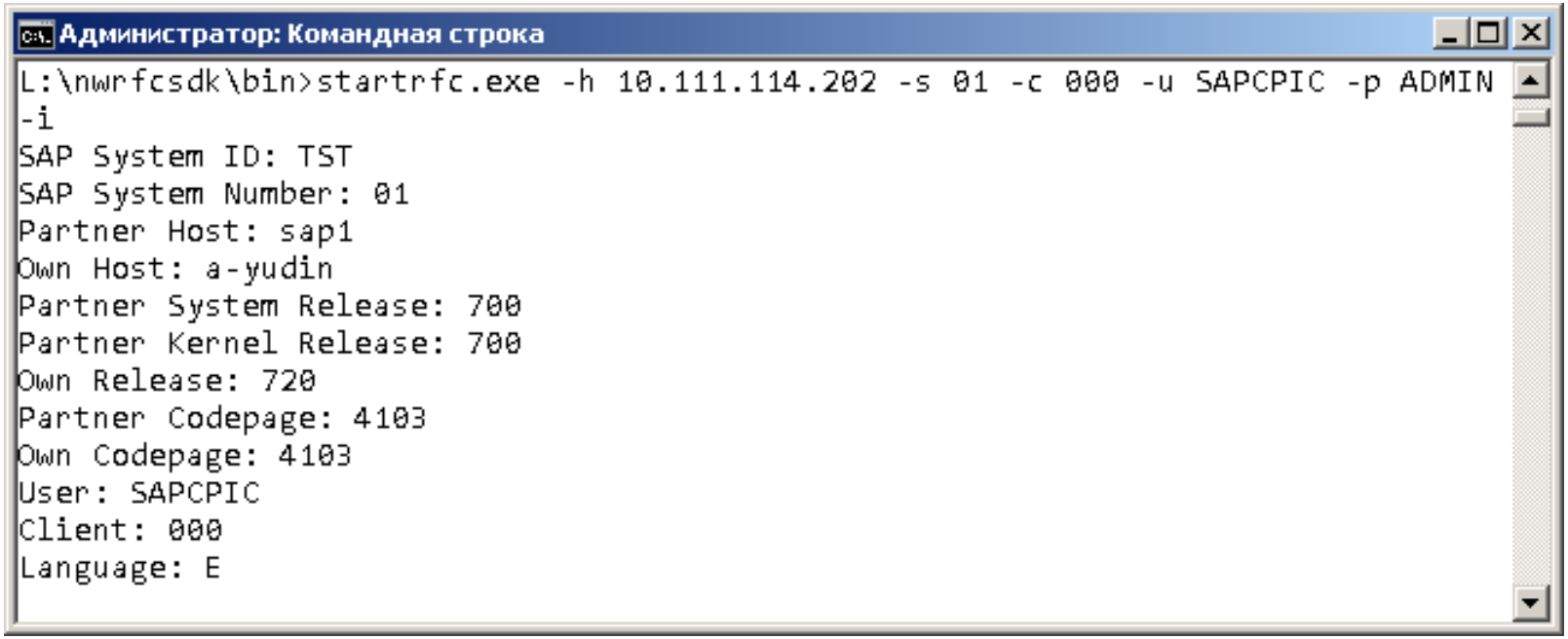
Подбор клиентов



Перебор паролей и пользователей



StartRFC.exe – успешное подключение



Pentest. Получение информации о системе

Vulnerability

Information Disclosure

ID: 8159

Short Description

Vulnerability allows remote attackers to obtain sensitive information.

Description

SAP allows remote attackers to obtain potentially sensitive information such as operating system and SAP version via an RFC_SYSTEM_INFO RfcCallReceive request, a different vulnerability than CVE-2003-0747.

System ID : TST
Protocol version : 011
Operating system : Windows NT
Central database : ORACLE
Database host : SAP2
IP address : 10.111.114.202
SAP kernel release : 700

Pentest. Проверка шифрования

Vulnerability

Insecure SAP RFC protocol

ID: 8163

Short Description

Login and password are sent in plain text.

Description

By default SAP RFC sends login as plain text and password is obfuscated by XOR with known fixed key. In case of traffic interception, attacker can get login and password.

Solution

Use SNC (Secure Network Communications) from SAP.

Pentest. Подбор клиентов

Information Available

Clients found

ID: 8138

Description

Available SAP clients found.

Available SAP clients

Availiable clients
000
001
066
800
810
811
812

Pentest. Подбор пользователей и паролей

High level

Account found

SAPCPIC

ID: 8136

Description

SAP account found. Unauthorized access is possible.

SAP account

Login	Password	Client	Status
SAPCPIC	SAPCPIC	000	Non-dialog user
SAPCPIC	SAPCPIC	001	Non-dialog user
SAPCPIC	SAPCPIC	800	Non-dialog user

Solution

Set a complex password for the user or block the user.

Audit. Анализ паролей по хешу

Серьезная уязвимость

Учетные записи с правами администратора с простыми паролями

ID: 178358

Описание

Учетные записи с простыми паролями и с правами администратора

Учетная запись	Пароль	Статус учетной записи	Профиль
SAP*	sap123456	не заблокирована	SAP_ALL

Рекомендации

- **Настроить профили безопасности в части парольной политики**
- **Периодически проверять пароли пользователей на наличие простых паролей**
- **Использовать таблицу запрещенных паролей USR40**
- **Запретить клонирование аутентификационных данных между системами**
- **Использовать шифрование между клиентами и серверами приложений**

Compliance

- **SAP Security guides – Password Policy**
- **Требования ISACA (Security, Audit and Control Features SAP ERP)**
- **Рекомендации DSAG (http://www.dsag.de)**
- **Рекомендации SAP Community Network (http://scn.sap.com/welcome)**

Спасибо за внимание!

Юдин Алексей

ayudin@ptsecurity.ru

POSITIVE TECHNOLOGIES