



onapsis
Securing Business Essentials

SAP® Penetration Testing

with Onapsis Bizploit

Mariano Nuñez Di Croce
mnunez@onapsis.com

April 22, 2010

HITB Security Conference, Dubai

Disclaimer

This publication is copyright Onapsis SRL 2010 – All rights reserved.

This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Who is Onapsis?

- Specialized company focused in **ERP Security** (**SAP**®, Siebel®, Oracle® E-Business Suite™, JD Edwards® , ...).
- Core business areas:
 - Development of specialized security software solutions.
 - Security consultancy services.
 - Trainings on business-critical systems security.

Who am I?

- **Director of Research and Development at Onapsis.**
- Degree in Computer System Engineering.
- Originally devoted to **Penetration Testing** and **Vulnerability Research**.
- Discovered **vulnerabilities** in Microsoft, Oracle, SAP, IBM, ...
- **Speaker/Trainer** at Black Hat, HITB, Sec-T, Hack.lu, DeepSec, Ekoparty..

Agenda

- The need for specialized ERP Security Assessments
- SAP Basics
- SAP Penetration Testing:
 - Discovery phase
 - Exploration phase
 - Vulnerability Assessment phase
 - Exploitation / Risk illustration phase
- Conclusions

The need for specialized ERP Security Assessments

Everything is about risk.

What is SAP?

- **Largest** provider of **business management solutions** in the world.
 - More than 140.000 implementations around the globe.
 - More than 90.000 customers in 120 countries.
- Used by **Fortune-500 world-wide companies**, **governmental organizations** and **defense facilities** to run their every-day business processes.
 - Such as Revenue / Production / Expenditure business cycles.

FINANCIAL PLANNING **TREASURY** **PAYROLL**

SALES **INVOICING** **LOGISTICS** **BILLING**

PRODUCTION **PROCUREMENT**

Insecure SAP Implementations == Insecure Business

- SAP Implementations are **long and complex** projects.
- The company goal's is to have the SAP system running by the deadline, **no matter what**.
- The SAP implementation-partner's goal is to set the SAP system running by the deadline, **no matter what**.
- Applying a holistic approach to **secure** the systems is usually regarded as an unnecessary **delay**...

Most SAP security settings are left by default

Many default settings are not secure

+

Many SAP systems out there are not secure

Some Facts and Thoughts...

- According to the FBI/CSI Computer Crime & Security Survey 2008, **financial frauds** caused by security incidents **costed US companies** an average of **USD 463,100**.
- **More than 95%** of the SAP implementations we have assessed, were **prone to financial frauds** derived from technical information security vulnerabilities.
- The biggest mis-conception in the term “SAP Security”: **SAP Security is much more than Segregation of Duties!**
 - Most standards & regulations still don't get it.
 - Most Auditing companies still don't get it.
 - Some customers still don't get it.

SoD is not enough to prevent attacks!

From the trenches:

During an assessment, a “SoD compliant” SAP system (which had cost \$\$\$\$^n to implement), could be remotely compromised in a matter of seconds through the exploitation of a vulnerability in a technological component.

Ok, but... which is the **real** risk?

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

ESPIONAGE

SABOTAGE

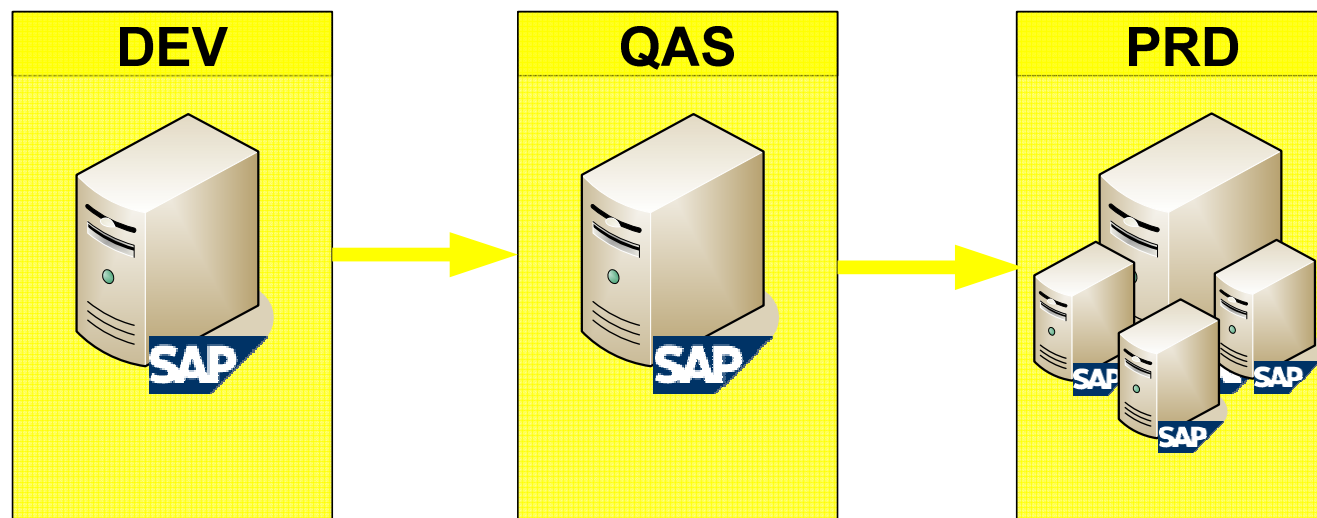
FRAUD

SAP Basics

Welcome to the SAP World

SAP Landscapes, Systems and Instances

- Typical SAP **Landspaces** are composed of three systems: Development, Quality Assurance and Production.
- Each system is build upon **one or more instances**.
- Systems are identified by **SAP System ID (SID)**.
- Each system (SID) is storing its information in its own Database.



■ Client (Mandant)

- Legally and organizationally **independent unit** in an SAP system (company group, business unit, corporation).
- Identified by a **three-digit number**.
- **Default clients**: 000, 001 and 066.

■ Reports / Programs

- ABAP programs that receive user input and produce a report in the form of an interactive list.

■ The RFC (Remote Function Call) Interface

- Used to call function modules **on remote systems**.

SAP Penetration Testing

How to do it

Hot news! Onapsis Bizploit

- First **Open-source ERP Penetration Testing Framework**.
 - Mainly focused in SAP right now.
 - Plugins for other ERPs coming soon! (awaiting patches ;)).
- Developed by the Onapsis Research Labs.
- Designed as a **proof-of-concept** and for academic research.
- **GPL and free**.
- Developed in Python and C.
- Command-line interface.
- Based on the *sapyto* GPL project.

*If you need a commercial-grade solution, ask me for **Onapsis One** later! (shameful advertisement).*

Onapsis Bizploit Architecture

- Core framework + plugins.
 - Discovery plugins
 - Vulnerability Assessment plugins
 - Exploit plugins

- Based on **connectors**:
 - SAP RFC Interface (Application Servers)
 - SAP RFC Interface (External Servers)
 - SAP Gateway
 - SAProuter
 - **SAP Enterprise Portal**
 - **SAP WebAS (ICM)**

Discovery Phase

Finding SAP targets

Discovering SAP Systems and Applications

- Available Options:
 - Traffic sniffing.
 - SAP portscanning.
 - Checking SAPGUI configurations.
- SAP Systems use a “fixed” range of ports.
- Most ports follows the PREFIX + SYS. NUMBER format.
- Common ports: 32XX, 33XX, 36XX, 39XX, 3299, 81XX, ...

Exploration Phase

Getting as much information as possible

Getting Information from SAP Application Servers

- The **RFC_SYSTEM_INFO** function module returns information about remote SAP Application Servers.
- Can be **called remotely** (and anonymously!) by default.

Remote System Information:

```
RFC Log Version: 011
Release Status of SAP System: 700
Kernel Release: 700
Operating System: Linux
Database Host: sapl01
Central Database System: ORACLE
Integer Format: Little Endian
Daylighth Saving Time:
Float Type Format: IEEE
Hostame: sapl01
IP Address: 192.168.3.4
System ID: TL1
RFC Destination: sapl01_TL1_00
```

Getting Information from SAP Application Servers

- The `RFC_SYSTEM_INFO` function module returns information about remote SAP Application Servers.
- Can be **called remotely** (and anonymously!) by default.

Protection / Countermeasure



- **Restrict connections to the Gateway at the network level.**
- **Protect against anonymous RFC calls**
- **For more information, refer to SAP Note 931252.**

```
Hostame: sap101  
IP Address: 192.168.3.4  
System ID: TL1  
RFC Destination: sap101_TL1_00
```

Discovering Available Clients

- There are some clients installed by default: 000, 001, 066.
- These clients are available in most SAP systems.
- After the installation, the administrator will install the *real* clients.
- It is possible to bruteforce the whole client-range to discover available ones.

Vulnerability Assessment Phase

Identifying security threats


SAP Default Users

- There is **public information** regarding the existence of **default SAP user accounts**.
- Many of these accounts are configured with **high privileged profiles**.

User ID	Description	Clients	Password
SAP*	Super user	000,001, 066 new clients	06071992 PASS
DDIC	ABAP Dictionary super user	000,001	19920706
EARLYWATCH	User for the EarlyWatch Service	066	SUPPORT
SAPCPIC	Communication User	000, 001	ADMIN

SAP Default Users

- There is public information regarding the existence of default SAP user accounts.
- Many of these accounts are configured with high privileged profiles.

User ID	Protection / Countermeasure 		
SAP*	<ul style="list-style-type: none">▪ Default users must be secured.▪ SAP* should be deactivated.▪ Use report RSUSR003 to check the status of default users.		
DDIC			
EARLYWA			
	EarlyWatch Service		
SAPCPIC	Communication User	000, 001	ADMIN

Assessing the RFC Interface

- The **RFC Interface** is the most widely used communication system in SAP landscapes.
 - Interfaces between SAP systems (internal or B2B)
 - Connections between SAP and external systems.
- By default, many of these interfaces are not properly secured.
- Practical example: the RFCEXEC server.

Exploitation / Risk illustration Phase

Letting people understand the Real risk

Showing that the risks are REAL

- It is easy for a **security-aware officer** to understand the risks by analyzing a vulnerability report.
- Anyway, dealing with false positives involves lot of effort (IT staff men-hours).

Getting the C-level involved...

- Financial officers do not understand technical vulnerabilities.
- Show them the **real risks!** -> Live-demos, screenshots of post-exploitation activities, etc.
- It is the only way to get them involved and **aware** of the threats they are facing.
- **They need to know the involved threats to manage risk efficiently!**

SAP Password Considerations & Cracking

- SAP has implemented different password hashing mechanisms.
- Passwords hashes are stored in table **USR02** (BCODE, PASSCODE) and **USH02**.

Code Vers.	Description
A	Obsolete
B	Based on MD5, 8 characters, Uppercase, ASCII
C	Not implemented
D	Based on MD5, 8 characters, Uppercase, UTF-8
E	Reserved
F	Based on SHA1, 40 characters, Case Insensitive, UTF-8
G	CODVN B + CODVN F (2 hashes)
H	Based on SHA1 with iterated salt
I	CODVN H + CODVN F + CODVN B (3 hashes)

- A patch for John the Ripper is available since June 2008!

SAP Password Considerations & Cracking

- SAP has implemented different password hashing mechanisms.
- Passwords hashes are stored in table USR02 (BCODE, PASSCODE) and USH02

Protection / Countermeasure



- Access to tables USR02 and USH02 should be protected.
- Password security should be enforced through profile configuration (login/* parameters).
- Table USR40 can be used to protect from trivial passwords.
- For more information, refer to SAP Note 1237762.

CODVN H + CODVN F + CODVN B (3 hashes)

- A patch for John the Ripper is available since June 2008!

Exploiting SAP/Oracle Authentication Mechanism

- Discovered by me in 2007.
- Discovered by Jochen Hein in 2002 (D'oh!)
- Target: Default SAP/Oracle installations.

The SAP+Oracle Authentication Mechanism

- SAP connects to the database as the OPS\$<SID>ADM (e.g: OPS\$PRDADM)
- Retrieves encrypted username and password from table SAPUSER.
- Re-connects to the database, using the retrieved credentials.

Exploiting SAP/Oracle Authentication Mechanism

- There is a special Oracle configuration parameter named **REMOTE_OS_AUTHENT**.
- If set to TRUE, Oracle “**trusts**” that the remote system has authenticated the user used for the SQL connection (!)
- The user is created as “identified externally” in the Oracle database.
- Oracle recommendation: **remote_os_authent = false**
- SAP **default** and **necessary** configuration: **remote_os_authent = true**
- **What does the attacker need?**
 - Database host/port.
 - SAP System ID.
 - Oracle Instance ID (= SAPSID?)

Exploiting SAP/Oracle Authentication Mechanism

- There is a special Oracle configuration parameter named **REMOTE_OS_AUTHENT**.
- If set to TRUE, Oracle “trusts” that the remote system has authenticated the user used for the SQL connection (!)
- The user is
- Oracle reco
- SAP default
- What does
 - Databa
 - SAP System ID.
 - Oracle Instance ID (= SAPSID?)

Protection / Countermeasure

Restrict who can connect to the Oracle listener:

```
tcp.validnode_checking = yes  
tcp.invited_nodes = (192.168.1.102, ...)
```

Remote Bizploit shells and Beyond

- Some bizploit **exploit plugins** can generate shells.
- For example, by abusing weak RFC interfaces, a **remote shell** can be spawned:

```
Starting EXPLOIT plugins
-----

rfcexec(target#1-3) {
    Trying to connect...
    Creating new SHELL...
    SHELL created.
} res: Ok
Finishing sapyto execution - Fri Apr 1 22:37:42 2009
sapyto> shells
sapyto/shells> show
Shell ID: 0 [RFCEXECShell]
    Target information (#1):
        Host: sap101

        Connector: SAPRFC_EXT
        SAP Gateway Host: sap101
    ...

sapyto/shells> start 0
Starting shell #0
    RFCEXECShell - Run commands & read files through rfcexec.
    The remote target OS is: Linux.
sapyto/shells/0> run whoami
    Command was run successfully.
    tlladm
```

Remote Bizploit shells and Beyond

- Some bizploit exploit plugins can generate shells.
- For example, by abusing weak RFC interfaces, a remote shell can be spawned:

Protection / Countermeasure



- Starting of External RFC Servers is controlled through the file specified by the *gw/sec_info* profile parameter.
- This file should exist and restrict access to allowed systems to start specific programs in the Application Servers.
- The *gw/reg_info* file protects Registered Servers and should also be configured.
- For more information, refer to SAP Note 618516.

```
Starting shell #0
RFCEXECShell - Run commands & read files through rfexec.
The remote target OS is: Linux.
sapyto/shells/0> run whoami
Command was run successfully.
tlladm
```

Conclusions

Wrapping up

Conclusions

- Weak SAP security drastically increases the probability of financial frauds and availability of the core business information.
- SAP provides several security features and protection against these attacks. However, implementations usually leave the system running, not secure.
- By default, many settings are not safe and are never changed.
- Segregation of Duties is absolutely necessary, but IT IS NOT ENOUGH! Many technical vulnerabilities allow remote attackers to take complete control of the business information (even without having an account in the system).

Conclusions

- The current **state-of-the-art** in the auditing of these systems is **far from being mature**. Many “compliant” systems are still prone to financial frauds caused by security breaches.
- A **Penetration Test of your SAP platform** will provide you with an objective knowledge of the current risk level of your core business platform, helping you optimize IT staff effort and **decrease business risks**.
- Onapsis **bizploit** can be used as a proof-of-concept, to illustrate some of the current threats an SAP platform is facing.

¿Questions?

mnunez@onapsis.com

Thank you!



www.onapsis.com