SAP Forensics

Detecting White-Collar Cyber-crime

Mariano Nunez
mnunez@onapsis.com
@marianonunezdc

Juan Perez-Etchegoyen
jppereze@onapsis.com
@jp_pereze

March 13th, 2013

Troopers Security Conference

Disclaimer

This publication is copyright 2013 Onapsis Inc. – 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.

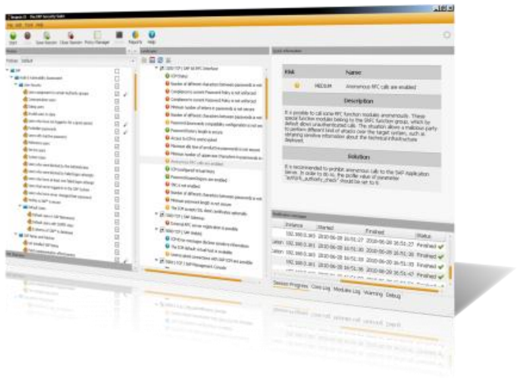
SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Who is Onapsis Inc.?

- Company focused in **protecting ERP systems from cyber-attacks**

(**SAP®,** Siebel®, Oracle® E-Business Suite^{TM}, PeopleSoft®, JD Edwards® …).

- Working with Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
  - Innovative ERP security software (Onapsis X1, Onapsis IPS, Onapsis Bizploit).
  - ERP security professional services.
  - Trainings on ERP security.



Who are we?

- **Mariano Nunez, CEO** at **Onapsis.**
- **Juan Perez-Etchegoyen, CTO** at **Onapsis.**
- **Ezequiel Gutesman** & **Nahuel Sanchez** from **Onapsis (Research Labs).**
- Discovered several **vulnerabilities** in SAP and Oracle ERPs...
- **Speakers/Trainers** at BlackHat, RSA, SAP GRC, HITB, Source, DeepSec...
- TROOPERS’ fans!

Agenda

- Introduction to SAP
- Forensics on SAP platforms
- Sample attacks and audit trails
- Conclusions

Introduction

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 **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes.**

BI ERP CRM BO PLM

PORTAL

SRM SCM SM PI GRC

Ok, so… what is SAP?

- In plain English: the systems that safeguard the **business crown jewels**.

PAYROLL

TREASURY

FINANCIAL PLANNING

BILLING

SALES

LOGISTICS

INVOICING

HUMAN RESOURCES

PRODUCTION

PROCUREMENT

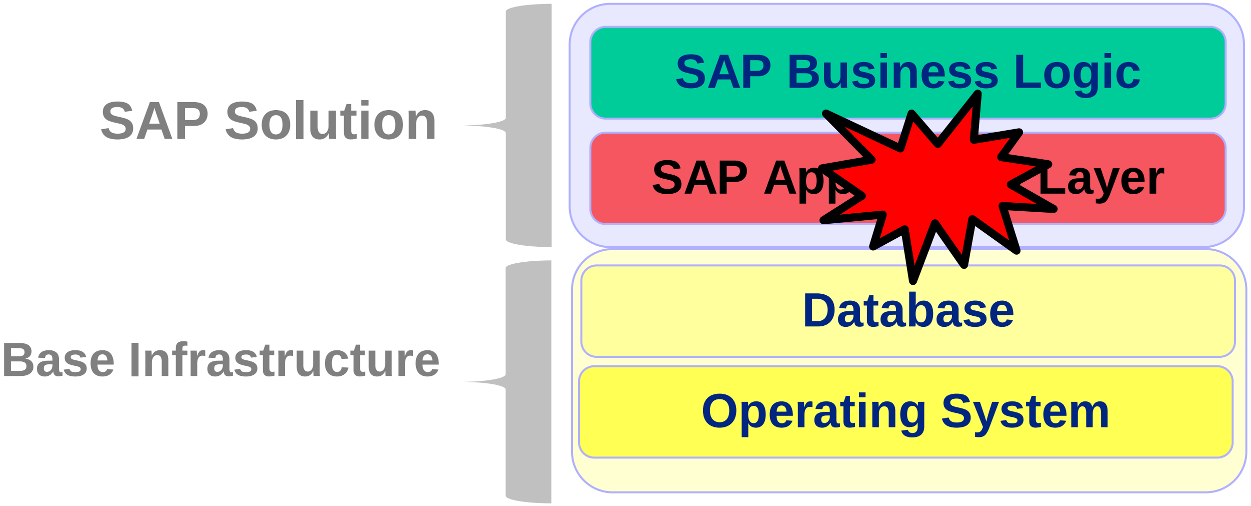
Cyber-attacks on SAP systems = $$$

- **If the SAP platform is breached**, an intruder would be able to perform different attacks such as:
  - **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
  - **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
  - **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

An attacker will exploit our Achilles' heel…

- SAP systems are built upon several layers.

- The SAP Application Layer (NetWeaver/BASIS) is common to most modern SAP solutions, serving as the base technological framework.



Note: The Database and Operating System layers should not be forgotten! Traditional techniques apply. Warning: reduced accountability due to SAP's using of single users (<sid>adm, SAPService<SID>, SAPR3,…)

Over 95% of the SAP systems we evaluated **were exposed to espionage, sabotage and fraud attacks** due to vulnerabilities in the SAP Application Layer.

Unlike SoD gaps, attackers do not need access credentials to exploit this kind of vulnerabilities…

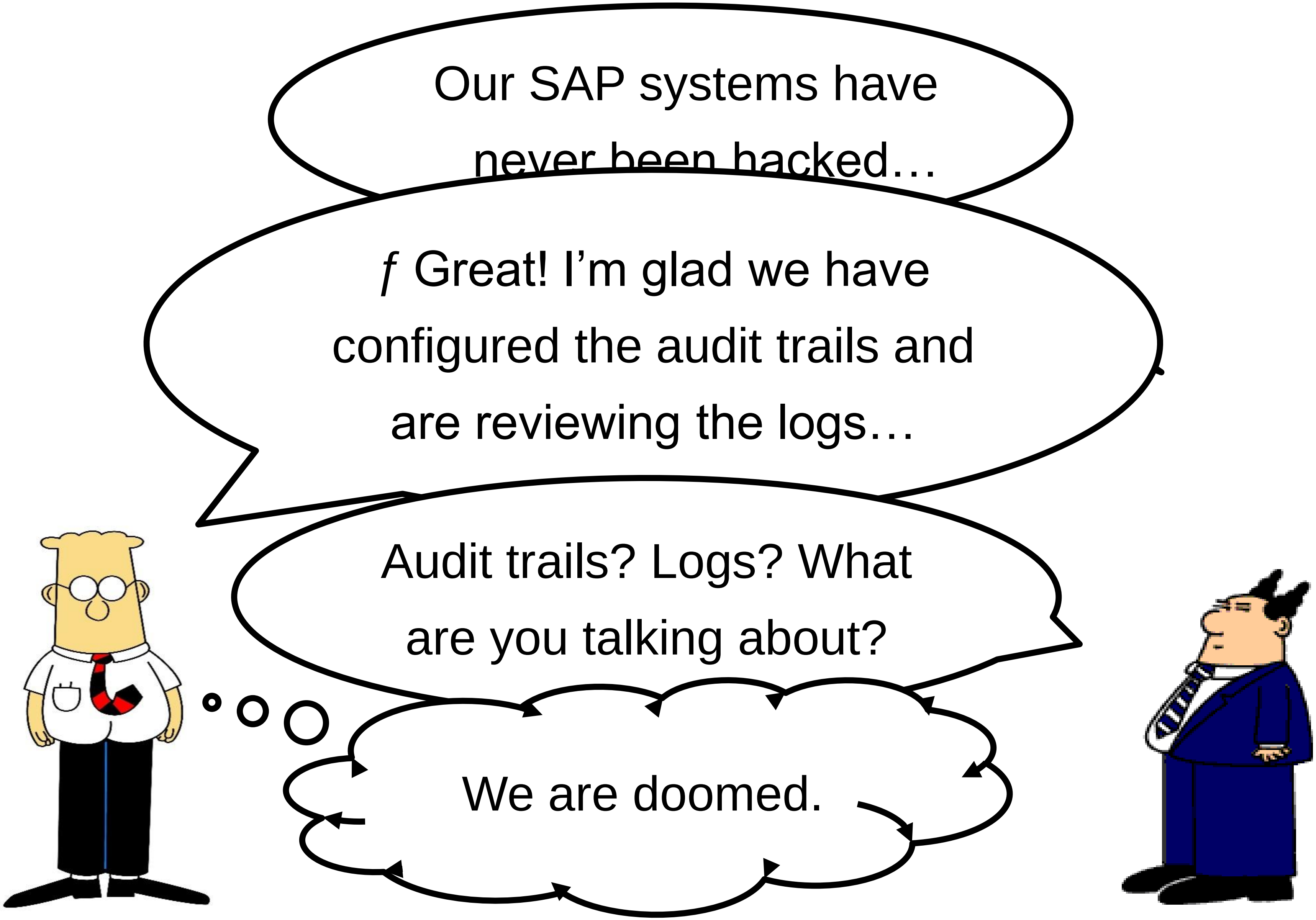
Forensics on SAP systems

Forensics & SAP

- According to Wikipedia "*Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and* ***investigation of material*** *found in digital devices, often in relation to* ***computer crime***".

- We are looking for an answer to these questions:
  - **Has my SAP platform been hacked?**
  - **Is it being attacked right now?**

We'll cover some of the standard capabilities provided in SAP systems to register evidence of user activity and/or attacks


Our SAP systems have never been hacked…
ƒ Great! I’m glad we have configured the audit trails and are reviewing the logs…
Audit trails? Logs? What are you talking about?
We are doomed.

On October 30th 2012, Anonymous claimed intent to exploit SAP systems

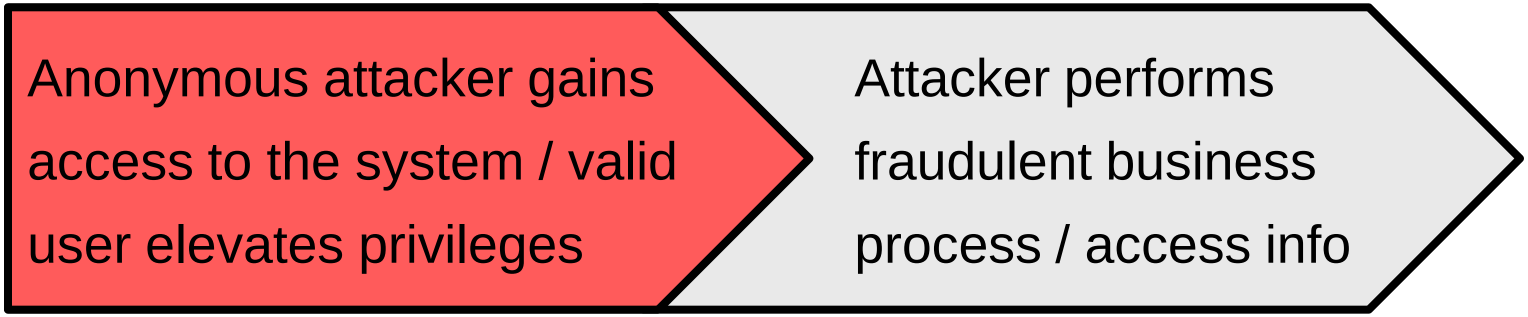
They claimed to have broken into the Greek Ministry of Finance (to be confirmed) and mentioned:

"We have new guns in our arsenal. A sweet 0day <u>SAP exploit</u> is in our hands and oh boy we're gonna sploit the hell out of it."

SAP Forensics & The Anatomy of an Attack

- Several SAP components are shipped with out-of-the-box capabilities to register user and technical activities.

- In this talk we will analyze the most important ones, describing their strengths, weaknesses and type of events that can be extracted from them, **following the "course of action" of a sample SAP attack**.



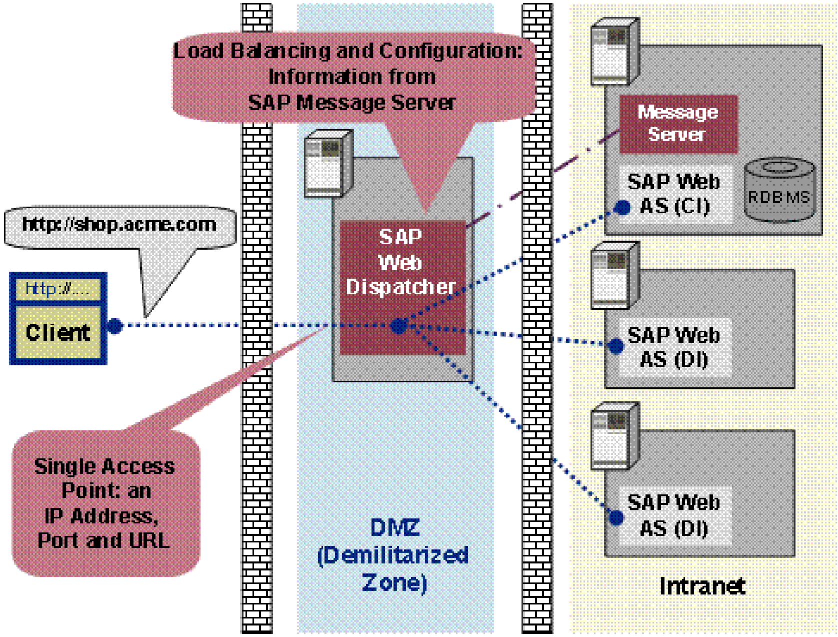
Anonymous attacker gains access to the system / valid user elevates privileges

Attacker performs fraudulent business process / access info

Initial Recon

The SAP Web Dispatcher

- The SAP Web Dispatcher is a reverse-proxy mainly used for load-balancing of HTTP(S) connections to SAP Web servers.
- It can also be used as a rudimentary Web Application Firewall.
- The Auditing and Tracing features also apply to the SAP Web Application Server (ICM).



Web Dispatcher – Security Log

Useful to detect the following events:

- HTTP fuzzing attempts
  - Null bytes in request
  - Bad protocol specification
- Incorrect logon attempts to Web administration interfaces

Information retrieved:

- Date & time
- Attacker’s source IP
- Request contents (depth defined by key **LEVEL**)

Web Dispatcher - Security Log: Summary

Description	Value
Enabled by default	WD: No ICM: Yes
Physical location of the log file(s)	WD: specified by admin ICM: /usr/sap/**<SID>**/**<INSTANCE>**/work/dev_icm_sec
Limit of the log file	Specified by **MAXSIZEKB** (kb) – Need SAP Note to work!
Action performed after reaching log limit	Defined by **FILEWRAP**
Centralized logging capabilities	No
How to access log(s) contents	WD: Operating system access ICM: Transaction MICM

Web Dispatcher – HTTP Log

Useful to detect the following events:

- Incorrect logon attempts (401 responses)
- HTTP fuzzing attempts (400 responses)
- Access to dangerous Web applications

Information retrieved:

- Request contents are determined by the **LOGFORMAT** key.
  - Date & time
  - Attacker’s source IP
  - User specified for authentication
  - HTTP Request parameters and headers
  - HTTP Response Code

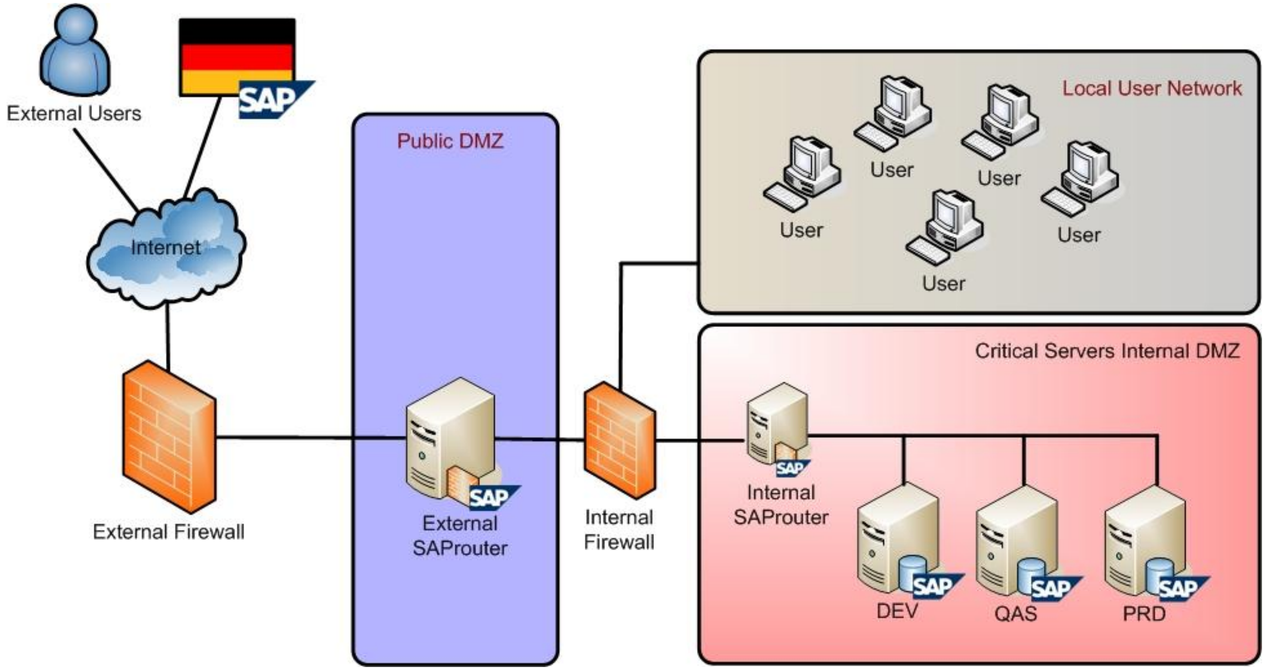
Web Dispatcher – HTTP Log: Summary

Description	Value
Enabled by default	WD: No ICM: No
Physical location of the log file(s)	Specified by parameter **icm/HTTP/logging_XX**
Limit of the log file	Specified by **MAXSIZEKB** (kb)
Action performed after reaching log limit	Defined by **FILEWRAP** and **SWITCHTF**
Centralized logging capabilities	No
How to access log(s) contents	WD: Operating system access ICM: Transaction MICM

The SAProuter

● The SAProuter is a reverse proxy used to *restrict* remote access to SAP platforms.

● Restrict connections through a firewall-like ACL file called *Route Permission Table.*



Threats Affecting SAProuters

- From the Onapsis Research Labs, we have researched on the following attack vectors over SAProuter systems:
  - Discovering established connections (connected clients & backend SAP servers).
  - **Performing *port-scans* of internal systems.**
  - Routing *native* protocols - proxying protocols such as SSH or HTTP and accessing internal services.

Detailed information about these risks and their mitigation techinques:

- *The "Securing the Gate to the Kingdom: Auditing the SAProuter" whitepaper*
- *The ERP Security Blog*

Attacks on SAProuter

Detecting Attacks on SAProuters

Regular connection (accepted)

```
Mon May 31 14:30:45 2010 CONNECT FROM C1/- host 192.168.0.1/43556
Mon May 31 14:30:45 2010 CONNECT TO S1/2 host 192.168.0.105/3200 (192.168.0.105)
Mon May 31 14:30:58 2010 DISCONNECT S1/2 host 192.168.0.105/3200 (192.168.0.105)
```

Regular connection (rejected)

```
Mon May 31 14:32:25 2010 CONNECT FROM C1/- host 192.168.0.1/44654
Mon May 31 14:32:25 2010 PERM DENIED C1/- host 192.168.0.1 (192.168.0.1) to 192.168.0.105/3201
Mon May 31 14:32:25 2010 DISCONNECT C1/- host 192.168.0.1/44654 (192.168.0.1)
```

Detecting Attacks on SAProuters

Info-request (accepted)

```
Mon May 31 14:33:13 2010 CONNECT FROM C1/- host 192.168.0.1/4218
Mon May 31 14:33:13 2010 SEND INFO TO C1/-
Mon May 31 14:33:13 2010 DISCONNECT C1/- host 192.168.0.1/4218 (192.168.0.1)
```

Info-request (rejected)

```
Mon May 31 14:34:54 2010 CONNECT FROM C1/- host 192.168.0.1/4218
Mon May 31 14:34:54 2010 PERM DENIED C1/- info request
Mon May 31 14:34:54 2010 DISCONNECT C1/- host 192.168.0.1/4218 (192.168.0.1)
```

Native connection

```
Mon May 31 14:51:38 2010 CONNECT FROM C2/- host 192.168.0.1/54650
Mon May 31 14:51:38 2010 CONNECT TO S2/1 host 192.168.0.105/22 (192.168.0.1), ***NATIVE
ROUTING ***
```

Detecting Attacks on SAProuters

Detecting Port-scanning Attacks

```
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56734
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3200
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56734 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56735
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3201
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56735 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56736
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3202
Wed Jun 30 22:28:16 2010 DISCONNECT   C1/- host 10.0.0.1/56736 (10.0.0.1)
Wed Jun 30 22:28:16 2010 CONNECT FROM C1/- host 10.0.0.1/56737
Wed Jun 30 22:28:16 2010 PERM DENIED  C1/- host 10.0.0.1 (10.0.0.1) to 192.168.3.2/3203
Wed Jun 30 22:28:17 2010 DISCONNECT   C1/- host 10.0.0.1/56737 (10.0.0.1)
…
```

The SAProuter Log: Summary

Description	Value
Enabled by default	No
Physical location of the log file(s)	Specified by the administrator through the –G option
Limit of the log file	None by default. Can be specified by option –J
Action performed after reaching log limit	If limit is defined, starts logging to a new file
Centralized logging capabilities	No
How to access log(s) contents	Operating system access

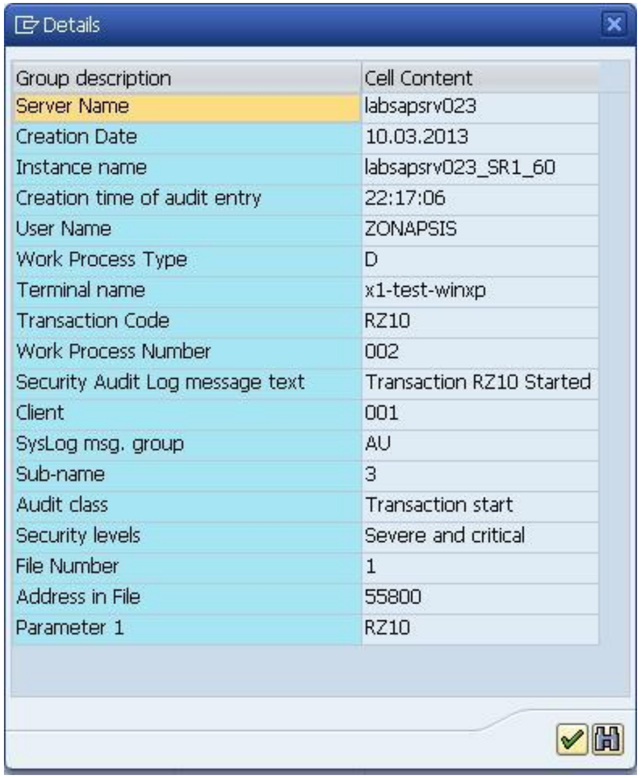
Bruteforce Attacks

ABAP – Security Audit Log

Security Audit Log (SAL) is **the** security auditing feature provided by SAP.

It enabled the identification of security-related events such as:

- Successful and unsuccessful dialog logon attempts
- Successful and unsuccessful RFC logon attempts
- RFC calls to function modules
- Changes to user master records
- Successful and unsuccessful transaction starts
- Changes to the SAL configuration



Group description	Cell Content
Server Name	labsapsrv023
Creation Date	10.03.2013
Instance name	labsapsrv023_SR1_60
Creation time of audit entry	22:17:06
User Name	ZONAPSIS
Work Process Type	D
Terminal name	x1-test-winxp
Transaction Code	RZ10
Work Process Number	002
Security Audit Log message text	Transaction RZ10 Started
Client	001
SysLog msg. group	AU
Sub-name	3
Audit class	Transaction start
Security levels	Severe and critical
File Number	1
Address in File	55800
Parameter 1	RZ10

Each event contains information about:

- Timestamp
- User, client and terminal (source system)
- Details of the activity performed

ABAP – Security Audit Log: Summary

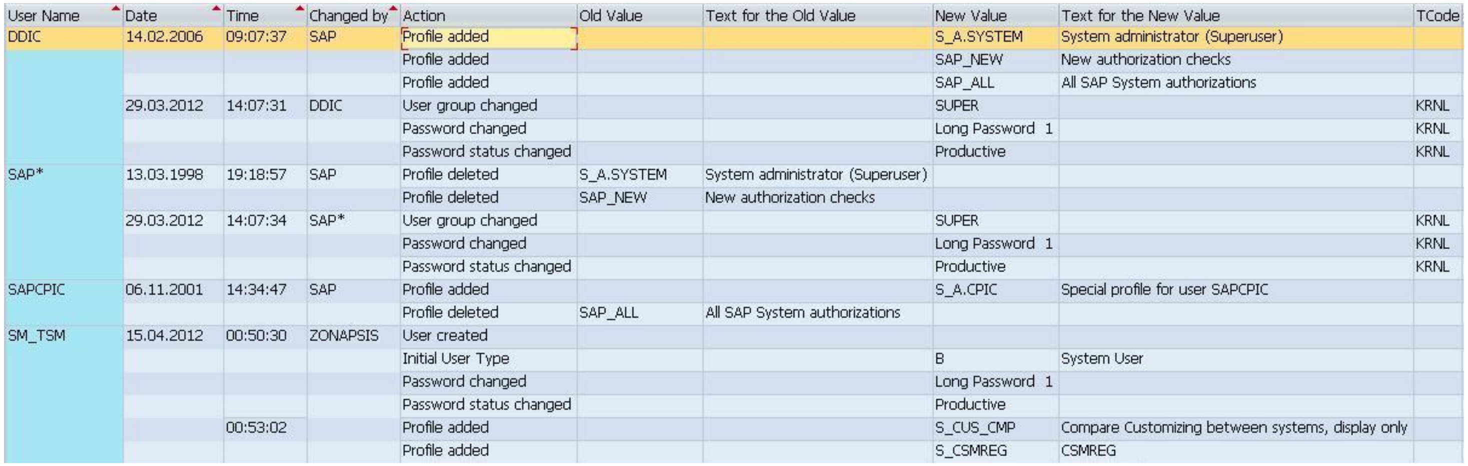
Description	Value
Enabled by default	No
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/log/audit_**date**
Limit of the log file	By default 20 Mb per audit file
Action performed after reaching log limit	Stops logging until next file is initialized (until the end of the day).
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction SM20

ABAP – User & Authorizations

The SAP system is configured by default to register all user and authorizations activity.

What kind of information will we get from the traces events?:

- Timestamp
- User who made the change
- Modified username and client (with the old and new values)
- Transaction/program



User Name	Date	Time	Changed by	Action	Old Value	Text for the Old Value	New Value	Text for the New Value	TCode
DDIC	14.02.2006	09:07:37	SAP	Profile added			S_A.SYSTEM	System administrator (Superuser)	
				Profile added			SAP_NEW	New authorization checks	
				Profile added			SAP_ALL	All SAP System authorizations	
	29.03.2012	14:07:31	DDIC	User group changed			SUPER		KRNL
				Password changed			Long Password 1		KRNL
				Password status changed			Productive		KRNL
SAP*	13.03.1998	19:18:57	SAP	Profile deleted	S_A.SYSTEM	System administrator (Superuser)			
				Profile deleted	SAP_NEW	New authorization checks			
	29.03.2012	14:07:34	SAP*	User group changed			SUPER		KRNL
				Password changed			Long Password 1		KRNL
				Password status changed			Productive		KRNL
SAPCPIC	06.11.2001	14:34:47	SAP	Profile added			S_A.CPIC	Special profile for user SAPCPIC	
				Profile deleted	SAP_ALL	All SAP System authorizations			
SM_TSM	15.04.2012	00:50:30	ZONAPSIS	User created					
				Initial User Type			B	System User	
				Password changed			Long Password 1		
				Password status changed			Productive		
		00:53:02		Profile added			S_CUS_CMP	Compare Customizing between systems, display only	
				Profile added			S_CSMREG	CSMREG	

ABAP – User & Authorizations: Summary

Description	Value
Enabled by default	Yes
Physical location of the log file(s)	Tables USH02, USH04, USH10, USH12…
Limit of the log file	No limit
Action performed after reaching log limit	N/A
Centralized logging capabilities	Not possible
How to access log(s) contents	Report RSUSR100N

ABAP – Table Change Logging

On SAP, all information is stored in tables and changes to these tables can reach the SAP system in two different ways:

- Changes performed by the system (rec/client)
- Changes performed through the transport system (recclient)

It is possible to restrict the client(s) and the **transparent** table(s) for which to log changes. All changes are saved into table **DBTABLOG,** containing:

- Timestamp
- User and client
- Table and field values (old and new)

ABAP – Table Change Logging: Summary

Description	Value
Enabled by default	No
Physical location of the log file(s)	Table DBTABLOG
Limit of the log file	No limit
Action performed after reaching log limit	N/A
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction SCU3

ABAP – Change Documents

- By default, the SAP system saves changes to the most important logical documents: Purchase Orders, Credit Cards, Vendor Information…
- It is possible for SAP customers to create their own change documents, registering changes to other documents.
- This type of logging can be very useful for "business-level" forensics.

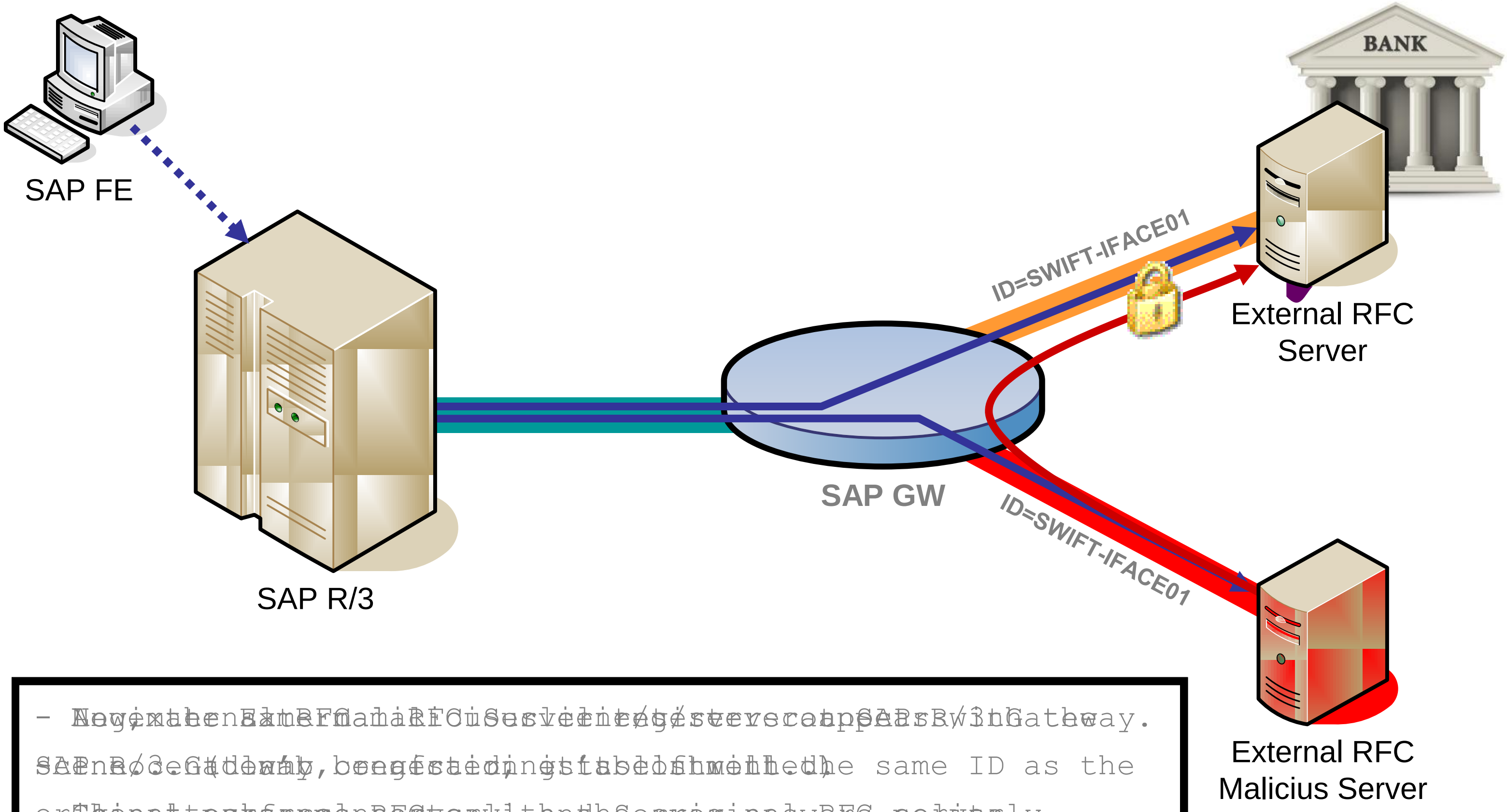
http://wiki.sdn.sap.com/wiki/display/CodeExchange/Use+of+Change+documents
http://help.sap.com/saphelp_nw70ehp2/helpdata/en/b8/686150ed102f1ae10000000a44176f/content.htm

ABAP – Change Documents: Summary

Description	Value
Enabled by default	Yes
Physical location of the log file(s)	Tables CDHDR, CDPOS
Limit of the log file	No limit
Action performed after reaching log limit	No limit
Centralized logging capabilities	Not possible
How to access log(s) contents	Report RSSCD200

Detouring Payments

Attacks on SAP Gateways – i.e. “EvilTwin”



- [illegible] Gateway.
[illegible] the same ID as the
[illegible] politely.
[illegible] attended
by the evil one.

Detecting Eviltwins on SAP Gateways

Gateway log:

```
S Wed Oct 10 2007 11:09:19:974 reginfo accepted server:
TP=IGS.WDFD00146227A, HOST=appserver01.company.com (10.18.94.4)


S Wed Oct 10 2007 11:10:24:975 reginfo accepted server:
TP=IGS.WDFD00146227A, HOST=appserver01.company.com (10.18.94.4)


S Wed Oct 10 2007 11:11:29:976 reginfo accepted server:
TP=SWIFT-IFACE01, HOST=swift.company.com (10.18.94.4)


S Sat Oct 13 2007 23:20:29:976 reginfo accepted server:
TP=SWIFT-IFACE01, HOST=101.205.120.45 (101.205.120.45)
```

Gateway Logging

Useful to detect the following events:

- Start of external RFC servers
- Registration of malicious RFC servers
- Execution of monitor commands
- Change in security configuration

Information retrieved:

- Request contents are determined by the **ACTION** key.
    - Date & time
    - Attacker’s source IP
    - Activity being performed (starting/registering server, monitor command being executed, etc)

Gateway Logs: Summary

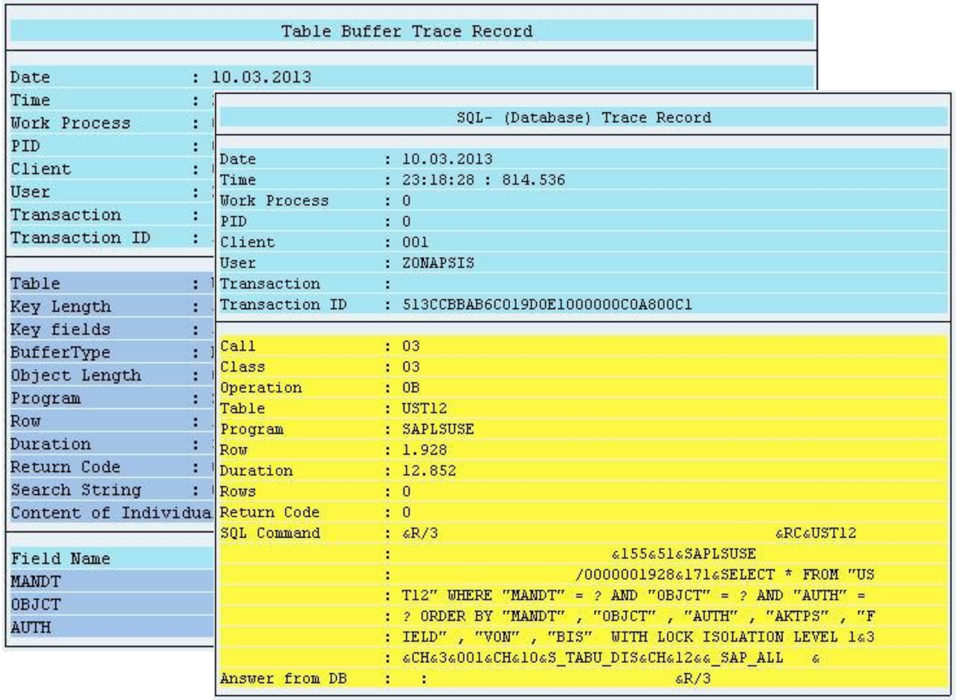
Description	Value
Enabled by default	No
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/work/<file_name> **<file_name>** is defined by key **LOGFILE**
Limit of the log file	Specified by **MAXSIZEKB** (kb)
Action performed after reaching log limit	Defined by **FILEWRAP** and **SWITCHTF**
Centralized logging capabilities	No
How to access log(s) contents	Transaction SMGW

Technical logs and traces

System Trace

The SAP system trace registers internal SAP activity such as database queries, authorization checks and execution of kernel and RFC functions, among other things.

- What kind of information do we get from the System Trace events?
  - Timestamp
  - Username and client
  - RFC/Table information
  - Transaction/program
  - Duration
  - Detailed individual fields



```
Table Buffer Trace Record

Date                 : 10.03.2013
Time                 :
Work Process         :
PID                  :
Client               :
User                 :
Transaction          :
Transaction ID       :

Table                :
Key Length           :
Key fields           :
BufferType           :
Object Length        :
Program              :
Row                  :
Duration             :
Return Code          :
Search String        :
Content of Individua

Field Name
MANDT
OBJCT
AUTH
```

```
SQL- (Database) Trace Record

Date            : 10.03.2013
Time            : 23:18:28 : 814.536
Work Process    : 0
PID             : 0
Client          : 001
User            : ZONAPSIS
Transaction     :
Transaction ID  : 513CCBBAB6C019D0E1000000C0A800C1

Call            : 03
Class           : 03
Operation       : 0B
Table           : UST12
Program         : SAPLSUSE
Row             : 1.928
Duration        : 12.852
Rows            : 0
Return Code     : 0
SQL Command     : &R/3                                    &RC&UST12
                :                          &155&51&SAPLSUSE
                :                      /0000001928&171&SELECT * FROM "US
                : T12" WHERE "MANDT" = ? AND "OBJCT" = ? AND "AUTH" =
                : ? ORDER BY "MANDT" , "OBJCT" , "AUTH" , "AKTPS" , "F
                : IELD" , "VON" , "BIS"  WITH LOCK ISOLATION LEVEL 1&3
                : &CH&3&001&CH&10&S_TABU_DIS&CH&12&&_SAP_ALL    &
Answer from DB  :   :                          &R/3
```

System Trace: Summary

Description	Value
Enabled by default	No. Activated upon user request
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/log/TRACE
Limit of the log file	By default: 16 Mb per file, 10 files = 160 Mb.
Action performed after reaching log limit	Overwrites the new files if limits are reached.
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction ST01 -> Analysis

Developer Traces

The developer trace is aimed to register technical activity of each SAP service. The information registered is highly-dependent on the service:

- RFC information
- Memory information
- Configuration information
- Error information

```
A Mon Mar 11 08:21:18 2013
A  *GENER* starting inline generation: /1BCDWB/DBUSH12
(reason: program touched by own LUW).
A
A Mon Mar 11 08:21:30 2013
A  *GENER* request remote generation: SAPICDT_.
A
A Mon Mar 11 08:21:47 2013
A  *GENER* starting inline generation: /1BCDWB/DBUSH04
(reason: program touched by own LUW).
A
A Mon Mar 11 08:26:13 2013
A  *GENER* request remote generation: SBAL_DISPLAY.
A  *GENER* request remote generation: SAPLSLG3.
M
M Mon Mar 11 08:49:23 2013
M  ThIUsrDel: th_rollback_usrdelentry = 1
```

```
======> CPIC-CALL: 'ThSAPOCMINIT' : cmRc=20 thRc=23
SAP gateway connection failed. Is SAP gateway start
ABAP Programm: /BDL/SAPLBDL11 (Transaction: )
Called function module: RFC_PING
User: ZONAPSIS (Client: 001)
Destination: SM_TSMCLNT001_BACK (handle: 7, , {513D
SERVER> RFC Server Session (handle: 1, 14445002, {5
SERVER> Caller host:
SERVER> Caller transaction code:  (Caller Program:
SERVER> Called function module: /BDL/RFC_CHECK
Error RFCIO_ERROR_SYSERROR in abrfcpic.c : 2323
CPIC-CALL: 'ThSAPOCMINIT' : cmRc=20 thRc=236
SAP gateway connection failed. Is SAP gateway started?
HOST =192.168.0.197
SERV =sapdp00
```

Developer Traces

The trace level is a numeric value that can be configured from different sources (even received remotely):

- Profile parameter rdisp/TRACE
- Configured on table RFCDES (T=Y)
- Profile parameters to accept remote trace (enabled by default)
  - rdisp/accept_remote_trace_level
  - gw/accept_remote_trace_level
- Environmental variables
  - CPIC_TRACE
  - RFC_TRACE
- Configured in the saprfc.ini or even at command line (-t)

[1] http://wiki.sdn.sap.com/wiki/display/ABAPConn/RFC+Trace+files+Increasing+in+Size
[2] https://service.sap.com/sap/support/notes/573800

Developer Traces

Each SAP service generates a trace file containing technical information

Component	File Name
Dispatcher	dev_disp
Work Process	dev_w<n> n is the work process number.
Dynp (screen processor), Roll, Paging, DB interface, ABAP processor, Enqueue (lock), Logging, Enqueue (lock), Logging	dev_dy<n>, dev_ro<n>, dev_pg<n>, dev_db<n>, dev_ab<n>, dev_eq<n>, dev_lg<n>, dev_eq<n>, dev_lg<n>
Message Server	dev_ms
SAPGUI (presentation)	dev_st<logon name>
APPC-server (CPIC gateway)	dev_appc
RFC (Remote Function Call) facility	dev_rfc, dev_rfc<n>
Gateway	dev_rd
R3trans and tp transport programs	dev_tp

Developer Traces: Summary

Description	Value
Enabled by default	Yes. TRACE level = 1
Physical location of the log file(s)	Depends on the service. Files are located in the following directory: /usr/sap/**<SID>**/**<INSTANCE>**/work/
Limit of the log file	By default: 16 Mb per file, 10 files = 160 Mb.
Action performed after reaching log limit	No limit if TRACE_LOGGING not active. 20 Mb by default per file.
Centralized logging capabilities	Not possible
How to access log(s) contents	Transaction ST11

SQL Audit

The SQL Audit logs all OPEN SQL **SELECT** statements to certain tables in dialog work processes.

The **statements** are written into sequential files in the file system of the application server.

The SQL Audit is not available from BASIS version 8.0 onwards.

There might be a considerable impact on performance (check SAP Note 115224).

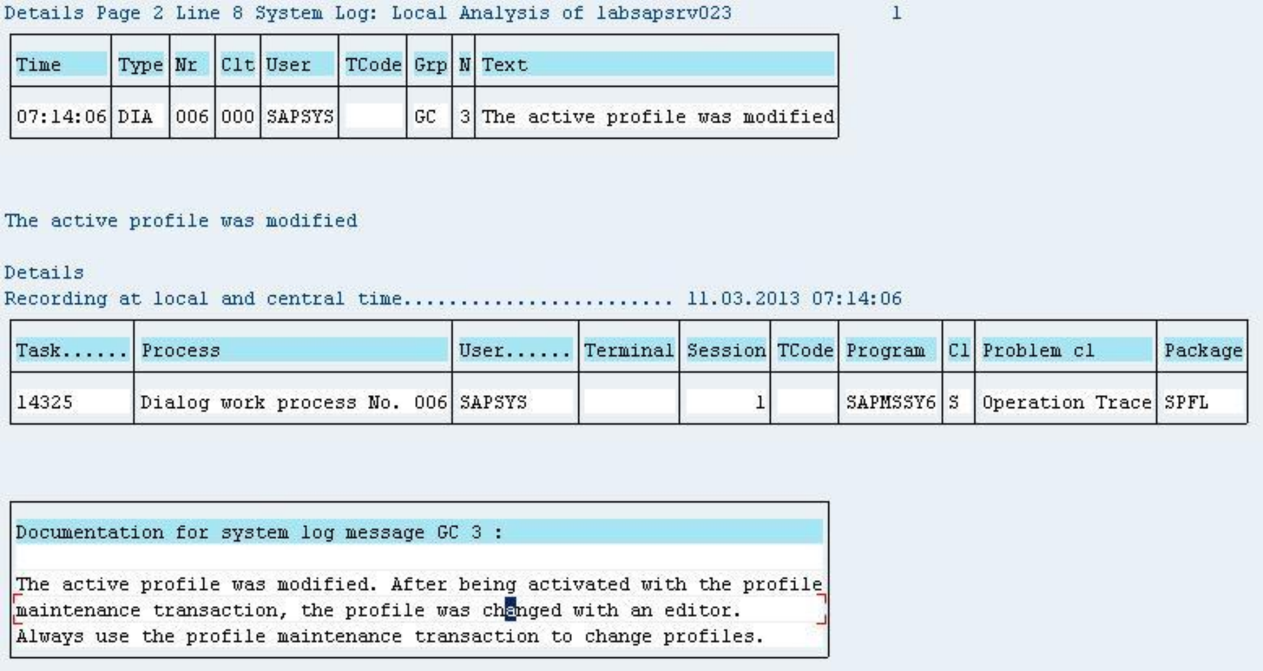
SQL Audit: Summary

Description	Value
Enabled by default	No
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/log/SQL_++++++++.AUD
Limit of the log file	By default 645 Mb (cd-rom size)
Action performed after reaching log limit	Creates a new file
Centralized logging capabilities	Not possible
How to access log(s) contents	No transaction available

System Log

From the SAP system log we can get technical information regarding program errors and problems containing:

- Client
- Username
- Transaction
- Program
- Error details



Details Page 2 Line 8 System Log: Local Analysis of labsapsrv023   1

Time	Type	Nr	Clt	User	TCode	Grp	N	Text
07:14:06	DIA	006	000	SAPSYS		GC	3	The active profile was modified

The active profile was modified

Details
Recording at local and central time........................ 11.03.2013 07:14:06

Task......	Process	User......	Terminal	Session	TCode	Program	Cl	Problem cl	Package
14325	Dialog work process No. 006	SAPSYS		1		SAPMSSY6	S	Operation Trace	SPFL

Documentation for system log message GC 3 :

The active profile was modified. After being activated with the profile maintenance transaction, the profile was changed with an editor. Always use the profile maintenance transaction to change profiles.

System Log: Summary

Description	Value
Enabled by default	Yes
Physical location of the log file(s)	/usr/sap/**<SID>**/**<INSTANCE>**/log/SLOG**<SYSNR>**
Limit of the log file	100000 = 1 Mb (specified by profile parameter rslg/max_diskspace/local)
Action performed after reaching log limit	Overwrites from the beginning
Centralized logging capabilities	Disabled by default. Not possible for Windows-based application servers
How to access log(s) contents	Transaction SM21

Conclusions

Conclusions

- It is impossible to cover this topic in a 1-hour talk! We had to leave several logging mechanisms out :(
- SAP is shipped with several features that can be used to support forensics analysis. However**, most of them are disabled by default** and must be explicitly enabled by the administrators.
- It is important to understand the limitations and characteristics of each feature to ensure we are logging the necessary information. Moreover, the performance impact of enabling them should be properly analyzed and understood.
- **If it is already difficult to know whether an SAP platform has been compromised, not recording user and technical activities makes it impossible.**

Questions?

Stay tuned!

@onapsis

@marianonunezdc

@jp_pereze

Thank you!