



onapsis
Securing Business Essentials



Hiding the breadcrumbs: Anti-forensics on SAP systems

Juan Perez-Etchegoyen

jppereze@onapsis.com

Will Vandevanter

wwandevanter@onapsis.com

March 2014

Troopers Security Conference

Disclaimer

This publication is copyright 2014 Onapsis, Inc. – All rights reserved.

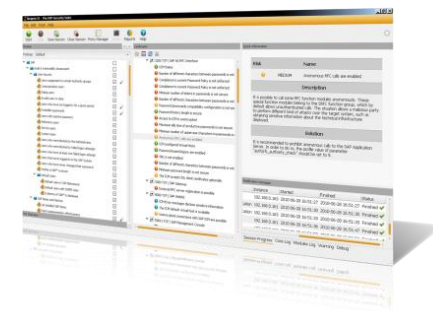
This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all 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™*, *PeopleSoft®*, *JD Edwards®* ...
- Trusted by Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
 - Innovative ERP security software (Onapsis X1, Onapsis Bizploit, Onapsis IA).
 - ERP security consulting services.
 - Trainings on business-critical infrastructure security.



Who are we?

- **Juan Perez-Etchegoyen, CTO at Onapsis.**
- **Will Vandevanter, Security Researcher at Onapsis.**

Agenda

- Introduction
- Anti-Forensic techniques
- Conclusions

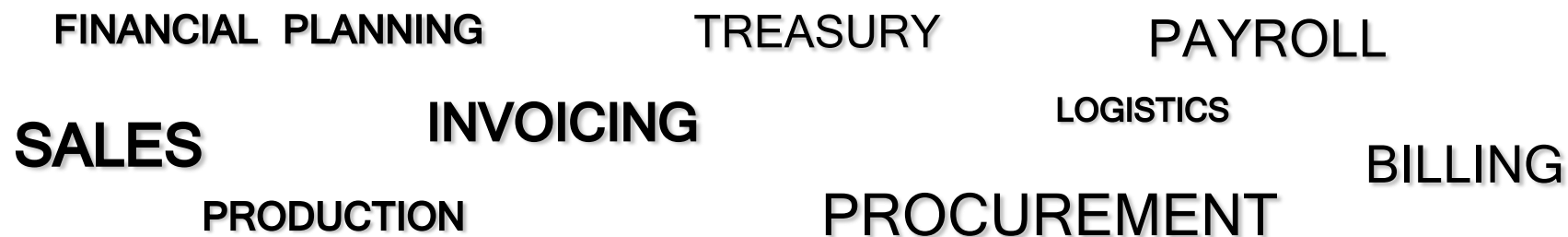
What should we expect out of this talk:

- Not a **full** anti-forensics guide.
- Shows several techniques taking advantage of current problems affecting logging mechanisms on SAP products.
- Follow-up of Troopers 2013 “SAP Forensics” talk.
- Not an hour talk.

Introduction

What is SAP?

- **Largest** provider of **business management solutions** in the world.
 - Hundreds of thousands of implementations and customers located all over the world.
- Used by **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes**.
 - Such as Revenue / Production / Expenditure business cycles.

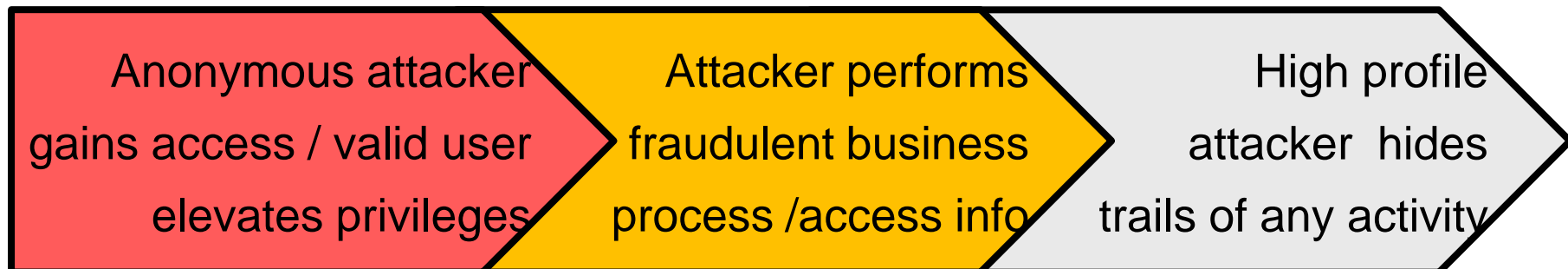


Over 95% of the SAP systems we evaluated **were exposed to espionage, sabotage and fraud attacks** due to vulnerabilities in the SAP Application Layer.

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

SAP Forensics & The Anatomy of an Attack

- Several SAP components are **shipped with out-of-the-box** capabilities to register user and technical activities.
- While in the previous talk we analyzed the most important ones, in this talk we will focus **on specific attacks** that might completely bypass some logging/auditing mechanisms



Forensics

- 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***”.
- Through Forensics, we are looking for an answer to these questions:
 - **Has my SAP platform been hacked?**
 - **Is it being attacked right now?**

The Security Audit Log



The *security audit log* can record the following security-related information:

- Dialog Logon attempts (successful and unsuccessful).
- RFC Logon attempts (successful and unsuccessful).
- Remote Function Calls.
- Transactions start attempts (successful and unsuccessful).
- Report start attempts (successful and unsuccessful).
- Changes to user master records.
- Changes to the auditing configuration.

SAL - Event Processing and Record Structure

- The audit log uses **filters**.
- Every time an event occurs, it is checked against defined filters.
- **If it matches, a log record is written to the audit file.**
- The log record has the following **structure**:
 - **Event identifier.**
 - SAP User ID and client.
 - **Terminal Name.**
 - Report Name.
 - Time and date.
 - Process ID.
 - Session Number.
 - Other information.
 - **Token: 2685-8765-2432-1790-3141**

Abusing of Security Audit Log

Attack #1 – Delete SAL messages

- Security Audit Log Events are shown through TX SM20
- The template messages are stored in table TSL1D
- User with only TCODE authorizations to SE92 can delete messages!
- This results in SAL events not being shown anymore (even though these are triggered).
- SAP Released Security Note 1926485 to fix this issue.

Any low-privileged user could delete SAL messages resulting in those messages not being unavailable for all users

Impact: Complete anonymity on any attack.

Attack #1 – Delete SAL messages

Data Browser: Table TSL1D Select Entries **36**

Table: TSL1D
Displayed Fields: 8 of 8 Fixed Columns: 2 List Width 0250

	AREA	SUBID	CLASID	SUBCLASID	SEVERITY	MONBEW	MONKAT	TXT
<input type="checkbox"/>	AU	0	X	1	2	GR	SH	Audit - Test. Text: &A
<input type="checkbox"/>	AU	1	X	2	5	YE	SH	Logon Successful (Type=&A)
<input type="checkbox"/>	AU	2	X	2	9	RE	SH	Logon Failed (Reason = &B, Type = &A)
<input type="checkbox"/>	AU	3	X	4	2	GR	SH	Transaction &A Started
<input type="checkbox"/>	AU	4	X	4	9	RE	SH	Start of transaction &A failed (Reason=&B)
<input type="checkbox"/>	AU	5	X	16	2	GR	SH	RFC/CPIC Logon Successful (Type = &A)
<input type="checkbox"/>	AU	6	X	16	9	RE	SH	RFC/CPIC Logon Failed, Reason = &B, Type = &A
<input type="checkbox"/>	AU	7	X	32	9	RE	SH	User &A Created
<input type="checkbox"/>	AU	8						
<input type="checkbox"/>	AU	9						
<input type="checkbox"/>	AU	A						
<input type="checkbox"/>	AU	B						
<input type="checkbox"/>	AU	C						
<input type="checkbox"/>	AU	D						
<input type="checkbox"/>	AU	E						
<input type="checkbox"/>	AU	F						
<input type="checkbox"/>	AU	G						
<input type="checkbox"/>	AU	H						
<input type="checkbox"/>	AU	I	X	64	9	RE	SH	Audit: Slot &A Inactive
<input type="checkbox"/>	AU	J	X	64	9	RA	SH	Audit: Active Status Set to &1
<input type="checkbox"/>	AU	K	X	128	2	GR	SH	Successful RFC Call &C (Function Group = &A)
<input type="checkbox"/>	AU	L	X	128	9	RE	SH	Failed RFC Call &C (Function Group = &A)
<input type="checkbox"/>	AU	M	X	2	9	RA	SH	User &B Locked in Client &A After Erroneous Password Checks
<input type="checkbox"/>	AU	N	X	2	9	RE	SH	User &B in Client &A Unlocked After Being Locked Due to Inval.Password Entered
<input type="checkbox"/>	AU	O	X	2	5	YE	SH	Logon Failed (Reason = &B, Type = &A)
<input type="checkbox"/>	AU	P	X	4	5	YE	SH	Transaction &A Locked
<input type="checkbox"/>	AU	Q	X	4	5	YE	SH	Transaction &A Unlocked
<input type="checkbox"/>	AU	R	X	32	5	YE	SH	&A &B Created
<input type="checkbox"/>	AU	S	X	32	5	YE	SH	&A &B Deleted
<input type="checkbox"/>	AU	T	X	32	5	YE	SH	&A &B Changed
<input type="checkbox"/>	AU	U	X	32	9	RE	SH	&A &B Activated
<input type="checkbox"/>	AU	V	X	1	9	RE	TP	Digital Signature Error (Reason = &A, ID = &B)

Attack #1 – Delete SAL messages

Data Browser: Table TSL1D Select Entries 36

Table: TSL1D
Displayed Fields: 8 of 8 Fixed Columns: 2 List Width 0250

	AREA	SUBID	CLASID	SUBCLASID	SEVERITY	MONBEW	MONKAT	TXT
<input type="checkbox"/>	AU	0	X	1	2	GR	SH	Audit - Test. Text: &A
<input type="checkbox"/>	AU	1	X	2	5	YE	SH	Logon Successful (Type=&A)
<input type="checkbox"/>	AU	2	X	2	9	RE	SH	Logon Failed (Reason = &B, Type = &A)
<input type="checkbox"/>	AU	3	X	4	2	GR	SH	Transaction &A Started
<input type="checkbox"/>	AU	4	X	4	9	RE	SH	Start of transaction &A failed (Reason=&B)
<input type="checkbox"/>	AU	5	X	15	2	GR	SH	RF515015 Logon Successful (Type = &A)

Protection / Countermeasure



- Implement SAP Security Note 1926485 (December 2013)
- Restrict S_DEVELOP authorization as those users could still delete messages.

<input type="checkbox"/>	AU	J	X	64	9	RA	SH	Audit: Active Status Set to &1
<input type="checkbox"/>	AU	K	X	128	2	GR	SH	Successful RFC Call &C (Function Group = &A)
<input type="checkbox"/>	AU	L	X	128	9	RE	SH	Failed RFC Call &C (Function Group = &A)
<input type="checkbox"/>	AU	M	X	2	9	RA	SH	User &B Locked in Client &A After Erroneous Password Checks
<input type="checkbox"/>	AU	N	X	2	9	RE	SH	User &B in Client &A Unlocked After Being Locked Due to Inval.Password Entered
<input type="checkbox"/>	AU	O	X	2	5	YE	SH	Logon Failed (Reason = &B, Type = &A)
<input type="checkbox"/>	AU	P	X	4	5	YE	SH	Transaction &A Locked
<input type="checkbox"/>	AU	Q	X	4	5	YE	SH	Transaction &A Unlocked
<input type="checkbox"/>	AU	R	X	32	5	YE	SH	&A &B Created
<input type="checkbox"/>	AU	S	X	32	5	YE	SH	&A &B Deleted
<input type="checkbox"/>	AU	T	X	32	5	YE	SH	&A &B Changed
<input type="checkbox"/>	AU	U	X	32	9	RE	SH	&A &B Activated
<input type="checkbox"/>	AU	V	X	1	9	RE	TP	Digital Signature Error (Reason = &A, ID = &B)

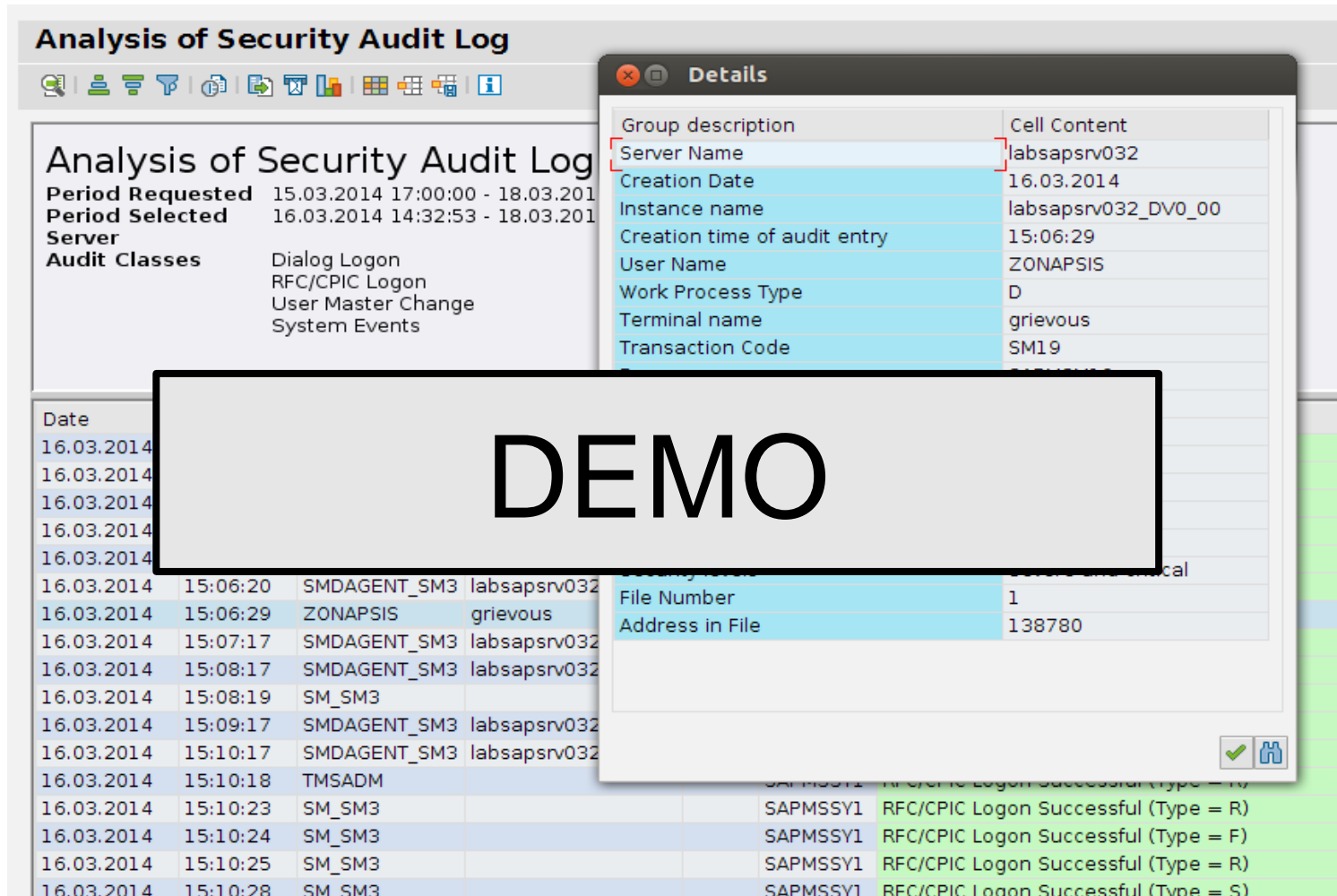
Attack #2 – Hide source of attack

- Security Audit Log Events have a unique field for the **source**
- By default the SAP App. Server makes a best effort to add the terminal name, but if not possible, then adds the IP address.
- Terminal name is data **provided by the client!**
- An IP address could be provided instead.
- Profile parameter **rsau/ip_only** is the only restriction for this attack (default value disabled)

The source for any (un)authenticated connection in the Security Audit Log cannot be trusted

Impact: Complete anonymity on the source of the attack.

Attack #2 – Hide source of attack



The screenshot displays the 'Analysis of Security Audit Log' interface. A large 'DEMO' watermark is centered over the main log table. A 'Details' dialog box is open, showing the following information:

Group description	Cell Content
Server Name	labsaprv032
Creation Date	16.03.2014
Instance name	labsaprv032_DV0_00
Creation time of audit entry	15:06:29
User Name	ZONAPSIS
Work Process Type	D
Terminal name	grievous
Transaction Code	SM19

The main log table shows the following data:

Date	Time	Work Process	Terminal	Transaction Code	Description
16.03.2014	15:06:20	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:06:29	ZONAPSIS	grievous		
16.03.2014	15:07:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:08:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:08:19	SM_SM3			
16.03.2014	15:09:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:10:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:10:18	TMSADM			
16.03.2014	15:10:23	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
16.03.2014	15:10:24	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
16.03.2014	15:10:25	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
16.03.2014	15:10:28	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = S)

Attack #2 – Hide source of attack

Analysis of Security Audit Log



Analysis of Security Audit Log

Period Requested 15.03.2014 17:00:00 - 18.03.2014
Period Selected 16.03.2014 14:32:53 - 18.03.2014
Server
Audit Classes Dialog Logon
RFC/CPIC Logon
User Master Change
System Events

Details

Group description	Cell Content
Server Name	labsaprv032
Creation Date	16.03.2014
Instance name	labsaprv032_DV0_00
Creation time of audit entry	15:06:29
User Name	ZONAPSIS
Work Process Type	D
Terminal name	grievous

Protection / Countermeasure



- Enable profile parameter **rsau/ip_only**
- Follow recommendations detailed in SAP Note **1497445**

16.03.2014					
16.03.2014	15:06:20	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:06:29	ZONAPSIS	grievous		
16.03.2014	15:07:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:08:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:08:19	SM_SM3			
16.03.2014	15:09:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:10:17	SMDAGENT_SM3	labsaprv032		
16.03.2014	15:10:18	TMSADM			
16.03.2014	15:10:23	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
16.03.2014	15:10:24	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
16.03.2014	15:10:25	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = R)
16.03.2014	15:10:28	SM_SM3		SAPMSSY1	RFC/CPIC Logon Successful (Type = S)

Attack #3 – Reaching the limit

- Limits are defined for the security audit log. By default no more than 100M of logs can be saved per day.
- Default behavior if the maximum size is reached is to **stop logging!**
- Some events can be triggered remotely and unauthenticated.
- If attacker knows what is being logged could potentially turn it off.

An unauthenticated user could disable the SAL if not properly sized by triggering events.


Impact: Complete anonymity on any attack.

Attack #3 – Reaching the limit

Security Audit: Display Configuration of All Instances

Static Configuratio DynamicConfigurati

Status of Recording on Individual Servers

Server Names	Release	Status	Current File Size	Maximum File ...
labsapsrv032 DV0 00	18.03.2014 20:50:07		112,000 MB	112,000 MB

DEMO

Filter 1 Filter 2

☒ Filter active

Selection criteria	Audit classes	Events
Client *	<input checked="" type="checkbox"/> Dialog logon	All
User *	<input checked="" type="checkbox"/> RFC/CPIC logon	
	<input checked="" type="checkbox"/> RFC call	
	<input checked="" type="checkbox"/> Transaction start	

Attack #3 – Reaching the limit

Security Audit: Display Configuration of All Instances



Static Configuratio

DynamicConfigurati

Protection / Countermeasure



- Perform a proper sizing of the Security Audit Log requirements to reduce the risk of reaching size limits.
- Send the alerts to an external source, potentially through CCMS.

✓ Filter active

Reset

Detailed Display

Selection criteria

Client

*

User

*

Audit classes

☒ Dialog logon

☒ RFC/CPIC logon

☒ RFC call

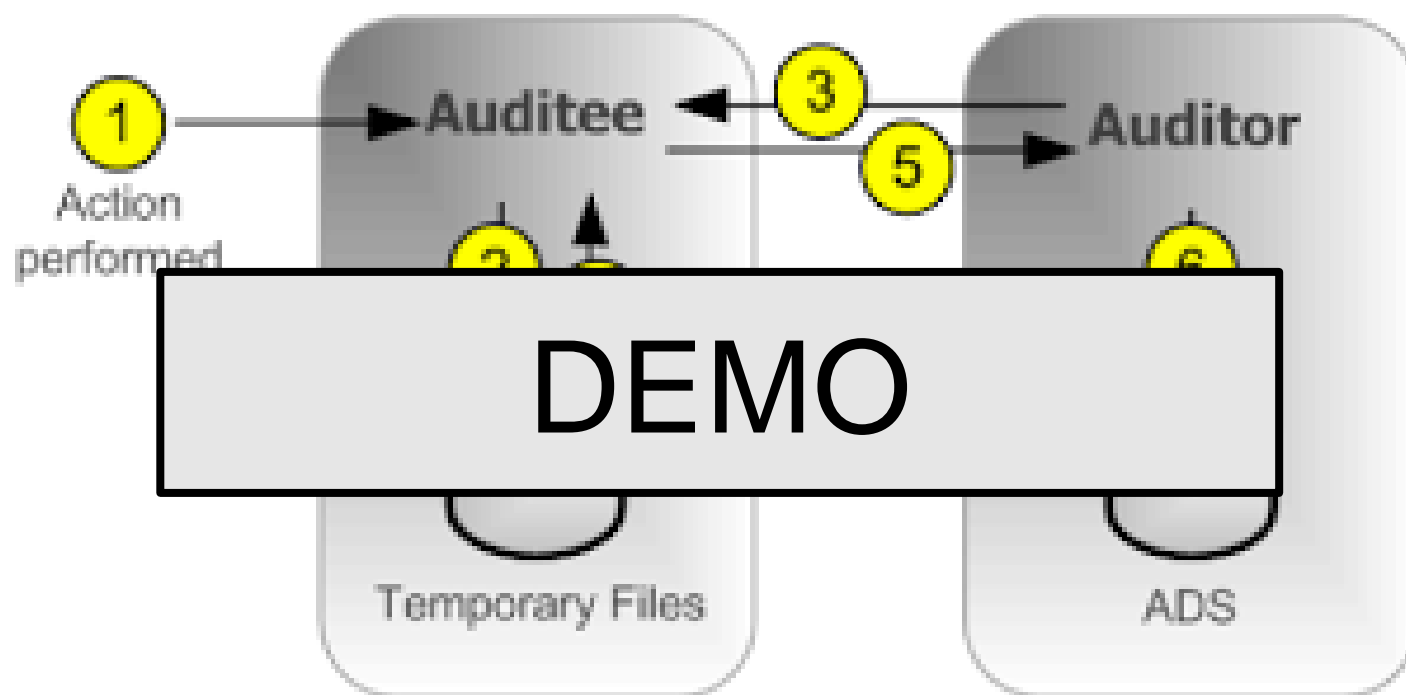
☒ Transaction start

Events

All

Attack #4 – SAP BO Temporary audit

Server auditing



NOTE: The Auditor and Auditee can also co-exist on the same CMS server.

Attack #4 – SAP BO Temporary audit

- BO architecture is distributed and by design there is a gap between when an event occurs and when it is written to the ADS
- This provides an attacker the opportunity to modify the event and hide actions
- No Integrity Check on the Temporary Files

Any user with filesystem access could delete temporary logs before reaching the ADS.

Impact: Complete anonymity on any attack.

Attack #4 – SAP BO Temporary audit

- BO architecture is distributed and by design there is a gap between when an event occurs and when it is written to the ADS
- This provides an attacker the opportunity to modify the event and

Protection / Countermeasure



- Protect Temporary Files at the OS level
- Correlate Events to detect anomalies

Any user with filesystem access could delete temporary logs before reaching the ADS.

Impact: Complete anonymity on any attack.

Locations

SAP Log and traces - Location

Logging mechanism	Location
Security Audit Log	/usr/sap/<SID>/<INSTANCE>/log/audit_date
Developer traces	Directory: /usr/sap/<SID>/<INSTANCE>/work/dev_*
System Log	/usr/sap/<SID>/<INSTANCE>/log/SLOG<SYSNR>
SQL Audit	/usr/sap/<SID>/<INSTANCE>/log/SQL_+++++++.AUD
System Trace	/usr/sap/<SID>/<INSTANCE>/log/TRACE
Gateway Log	/usr/sap/<SID>/<INSTANCE>/work/<file_name> <file_name> is defined by key LOGFILE
Web Dispatcher Log	Specified by parameter icm/HTTP/logging_XX
WD Security Log	/usr/sap/<SID>/<INSTANCE>/work/dev_icm_sec
Table Change Logging	Table DBTABLOG
User & Auth.	Tables USH02, USH04, USH10, USH12...
ABAP Change Doc.	Tables CDHDR, CDPOS

Recommendations and conclusions

General recommendations

- Enable logging and tracing mechanisms according to business requirements
- Enable technical logs too.
- Send the logs to a centralized facility
- Periodically review all logs
- Implement SAP Security Notes on all SAP systems to mitigate the risk of new vulnerabilities, specially the ones affecting the audit and logging mechanisms.
- Secure the profile parameters and the configuration of the SAP systems.
- Perform a proper sizing of the logging and tracing mechanisms to avoid reaching the defined limits.



RECOMMENDED

Conclusions

- It is important to understand the limitations and features of each logging and tracing mechanism to ensure we are logging the necessary information.
- If an attacker gets SAP_ALL or equivalent privileges and the logs were not sent to an external system, then no auditing or logging feature is reliable.
- **If it is already difficult to know whether an SAP platform has been compromised, not PROPERLY recording user and technical activities makes it impossible.**

References

- SAP Note **539404** - FAQ: Answers to questions about the Sec. Audit Log
- SAP Note **1497445** - SAL| Logging the IP instead of the terminal name
- SAP Security Note **1926485** - Missing authorization check in application "Edit System Log and Security Audit Log Messages"
- <http://scn.sap.com/thread/3298688>
- Troopers 2013 – “Detecting white-collar cybercrime: SAP Forensics”
- <http://www.onapsis.com>
- Special Thanks to the Onapsis Team :
 - Sergio Abraham
 - Nahuel Sanchez
 - Alex Horan

Questions?

jppereze@onapsis.com

wvandevanter@onapsis.com

Thank you!



www.onapsis.com

Follow us!  *@onapsis*