Webpage: www.ijaret.org
Volume 4, Issue I, Jan. 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

SAP ERP Forensics

Goraksh Shinde[1]

[1]Northeastern University, College of Computer and Information Science
360 Huntington Ave, Boston, Massachusetts 02115, United States
gorakshshinde@ccs.neu.edu, gorakshshinde@gmail.com

Abstract: *SAP ERP systems are the most important systems for the organizations that run on SAP platforms as it carries all the financial and business transactions information. SAP systems needs to be ready for Forensic Analysis and the applications like SAP Fraud Management can help tremendously in SAP ERP system forensics. SAP ERP systems are very tightly integrated thus finding and correlating incident data in SAP applications, SAP security audit logs and other sources of information is resource intensive. For proper SAP forensics analysis, business and financial processes understanding is important before analyzing audit log and change documents. In this paper, SAP ERP forensics analysis approach and methods are discussed to make full utilization of technical features provided by SAP platform.*

Keywords: *ERP, Fraud Management, Forensic Analysis, Security Audit, Business Processes, Change Documents.*

1. INTRODUCTION

Enterprise Resource Planning (ERP) is a system which integrates databases and applications for managing business processes and people within organization. There are few leading ERP providing firms like SAP, Oracle, PeopleSoft, J D Edwards etc. [5].

SAP ERP previously named as SAP R/3 is software that supports all the business processes like human resources, finance, operations, sales etc. These systems can be customized as per the industry requirements in healthcare, manufacturing, retail and insurance. SAP ERP Operations include functions like Sales and Distribution (SD), Materials Management (MM), Production Planning (PP), Logistics execution (LE), Quality Management (QM). These SAP operations communicate with the SAP ERP financials that includes Financial Accounting (FI), Management Accounting (CO) and Financial Supply Change Management (FSCM). Besides SAP ERP Human Capital management deals with the people working for an organization. SAP ERP systems are very tightly integrated thus finding and correlating incident data in SAP applications, SAP security audit logs and other sources of information is resource intensive. For proper SAP forensics analysis, business and financial processes understanding is important before analyzing audit log and change documents [1].

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.”

Computer forensics is the branch of forensics that deals with strategic gathering and analysis of the data in the computer realm which can be useful in legal proceedings. As far as ERP systems are concerned forensics analysis is not only limited to computer forensics but it also involves forensic accounting as ERP system deals with financial transactions in the system [6].

"Forensic Accounting is the integration of accounting, auditing and investigative skills which provides an accounting analysis that is suitable to the court which will form the basis for discussion, debate and ultimately dispute resolution [31].”

In SAP ERP forensics, SAP front end portal is very critical because it is directly exposed to the internet and provided it is connected to critical backend data systems, an attack can start from SAP front end portal to gain access of critical data in the backend system. The attacks on SAP front end portal can be tracked from the standard HTTP logs and POST request. HTTP logs will be helpful in analyzing the simple attacks and they cannot track complex attacks, complex attacks can be tracked and analyzed using POST requests [2].

ERP systems are based on database that is used by multiple business applications like business intelligence systems, employee benefits, payroll, insurance etc. and these applications can often share the data with the outside systems where there is no control of the administrator like some third party systems for employee benefits. Hence there are high chances that critical data can be shared in unsecure environment. Database forensics can also be critical during the Intellectual property, patent infringement cases, corporate espionage, virus infection etc. Forensic analysis in database can lead to further investigation in laptops, phones or other computer forensics related systems [8].

2. NEED FOR SAP ERP FORENSICS

2.1 SAP ERP Systems

SAP is a largest business process management solutions provider in the world. SAP ERP forensics is the need for organizations after recent anonymous attacks on ERP systems. No matter how much secure your ERP system is, it can be attacked by internal or external threats. Thus it is important to analyse those incidents in order to prevent them in future. There are multiple ways in which logs can be recorded in SAP ERP systems like HTTP log, security audit log, table access log, message server log, SAP gateway access log. It has been more apparent that most of the organizations do not use these features provided by ERP vendors and even if they are implemented, very few organizations collect them in a central storage in order to prevent them from attackers [2].

2.2 SAP ERP Vulnerabilities

SAP ERP forensics will help the organizations to find out whether there have been any previous attacks on the ERP system in the past and will also let us know whether the ERP system has been compromised.

1. SAP RFCs

In order to communicate with SAP instances, External servers register with SAP Gateway to communicate over SAP RFC protocol. RFC protocol supports bidirectional mode i.e. it will use already established connection thus it does not require separate authentication requirement as the original call was from SAP instance. If SAP system has existing connection with external RFC then it can be used to send information to different entities [9].

All SAP NetWeaver applications like ABAP development tools, HANA studio, RFC SDK, SAP GUI are vulnerable for remote exploitation. Attacker can gain access to NetWeaver services like dispatcher and gateway as these services are not encrypted hence man-in-the-middle attack can be conducted on such services by injecting malicious packets. Attackers can also disturb the SAP operations through denial of service attacks.

2. SAP web dispatcher

SAP NetWeaver 'Diag TraceR3Info' vulnerability arises when disp+work.exe module processes a specially crafted packet. This vulnerability allows attacker to remotely execute the arbitrary code with user privileges under dispatcher service. 'DiagTraceHex' and 'DiagTraceAtoms' vulnerabilities causes denial of services with remote authentication vulnerability [3].

3. SAP routers

SAP routers are application level gateways that are used to connect systems in SAP infrastructure. SAP routers allow connections on the basis of route permission table and if the table contains the password then it matches it with the password entered by the user. If the entered password is wrong then the password comparison function interrupts the evaluation cycle which can make attacker to perform timing attack [4].

4. SQL injection attacks

There can be native SQL injection vulnerability in SAP systems which can grant access of SAP_ALL in the SAP system to attacker. ABAP uses database through open SQL layer which is more secure than another database access layer provided by SAP called ABAP database connectivity (ADBC). ADBC allows any commands on database and chaining of multiple commands in a single call; it also allows assembling the command at runtime and does not restrict the database command to the client making it vulnerable to SQL injection attack [30].

5. Brute force attacks

SAP username and password can be attacked with brute force attack through SAP web GUI service. Default combinations of user id, password can be hacked by setting DEFAULT_CRED variable to be true and the path that stores these default combinations is MSF_DATA_DIRECTORY/wordlists/sap_default.txt [25].

6. Detouring payments

An attacker can detour the payments by gaining the admin access to check the vendor and bank details history to detour the payments.

2.3 Cyber-attacks on SAP ERP systems

On October 30th, 2012 anonymous claimed that they have hacked Greek ministry of Finance, They quoted, "We gained full access to the Greek Ministry of Finance. Those funky IBM servers don't look so safe now, do they..." Anonymous claimed to have SAP zero-day exploit.

Zero-day vulnerability is an unauthorized entry already available in the software which is not known to the software vendor and this entry can be exploited by hackers before it is identified by the vendors in order to fix it. This type of attack is zero day attack [24].

Attacker can gain access to the SAP ERP system and perform fraudulent business transactions.

SAP Security is not only limited to segregation of duties (SOD) now, as the complex business infrastructure framework remains susceptible to exploitation. Exploitation of such vulnerabilities can be used to perform malicious attacks like sabotage, espionage and fraudulent attacks to the business of an organization. The main difference between business infrastructure attack and segregation of duties attack is that in business infrastructure attack the attacker does not need any valid user account to target the SAP system and such vulnerabilities would allow complete control over the SAP system which can go undetectable during audit activities [14].

Most of the SAP systems are prone to following cyber-attacks [23]

1. Espionage- Espionage means obtaining confidential information without the permission of the owner of information.
2. Sabotage- Sabotage deals with defacement, destruction or tampering of the information or its assets of an organization.
3. Fraud- Fraud is wrongful use of the resources for monetary gain or benefits.

"Breaches are happening every day but still many CISOs don't know because they don't have visibility into their SAP applications," said Mariano Nunez, CEO and co-founder of Onapsis [26].

As per SAP insider, "74% of world's transactions are managed by SAP systems." SAP systems are very complex to implement due to tight integration of distinct business processes in it. SAP systems can possess vulnerabilities like source code vulnerability, RFC gateway vulnerability, default or weak passwords, missing kernel and patch upgrades, vulnerable third party add-ons, direct table access and critical access to users. These are some possible vulnerabilities that can be exploited by remote code execution, remote OS command execution and RFC gateway attack etc. [7].

US Investigation Services (USIS) was attacked through SAP vulnerability in 2013 through a third party managed environment which compromised the personal records of federal employees and contractors who had access to classified intelligence [13].

If the remote ABAP code execution is successful then attacker could check SAP financial transactions of the victim by running FK02 transaction and make the account number changes in it for fraudulent activities. Credit card information is used in many modules like sales and distribution, finance and there are more than fifty tables in SAP systems which contains credit card information. Remote function call can be exploited by using

RFC_READ_TABLE function, which allows checking content of tables [23].

'Sapsucker' is a tool that allows system access via RFC and HTTP. It involves reuse of logon cookies which can extract the sensitive data. However critical data can be encrypted through function modules like CCARD_DEVELOPE and CCSECA_CCNUM_DECRYPTION.

RFC destinations should be registered to prevent the SAP systems from such attacks. SAP J2EE user management can be exploited to create backdoors and through this, access to SAP portals and process integrations platforms can be gained for malicious activities. SAP RFC gateway can be exploited to modify the information in the database [26].

3. SAP ERP SYSTEM FORENSIC ANALYSIS

3.1 Forensics on SAP ERP Systems

As a computer forensics investigator, once you know that ERP system has been hacked you will have to trace back how it has happened what is the extent of damage. Forensics on ERP systems is not a straightforward task as it requires advanced skills and techniques in order to collect the volatile and non-volatile data for evidence extraction. Forensics investigator will extract the evidence, preserve it, maintain chain of custody for all the evidence and report it to law enforcement [29].

ERP system contains lot of business critical data and if it has been compromised then organization wants to keep their intellectual property safe from their competitors as once the matter is in court, all the information presented in court becomes available to general public as per federal laws.

3.2 Evidence Extraction

Once it has been identified that system has been compromised, first thing that needs to be done is to verify that the incident has occurred.

"In forensic science, Locard's exchange principle holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it and both can be used as forensic evidence [29]"

While performing incident response on live systems, system and data will keep on changing and evidence can be found out from different places like network, logs, databases and applications [29].

SAP ERP system contains various logs as below

1. Users and authorizations logs- User and authorization changes are logged in transparent tables in the database. Access to these tables is restricted through authorization control. These logs can be accessed through SUIM or SU01 transaction. It will give the information about user account activities and authorization changes. Critical information like user password is represented as hashed value [16].

2. Security audit logs- Security audit logs can be recorded in SAP ERP systems which stores information like 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 transactions hits and changes to audit configuration. Security audit log parameters are available as per below and can be set using transaction SM19. These parameters can be displayed using SM20 and deleted using SM18 [15].

3. Table change logs-Table change logs can be set using rec/client parameter and in log data changes flag through SE13. If both the things have been set then database logs table changes in the table DBTABPRT [16].

4. Change documents- Other change documents related to user, profiles, role and authorizations can be accessed through SUIM change documents.

5. SQL audit- SQL Audit logs all OPEN SQL SELECT statements but it requires large disk space which affects the system performance. It requires defining the number range for SQL audit files and required tables for which SQL statements needs to be logged. SQL audit requires setting up of below parameters.

1. rsau/SQL-Audit/switch – On/Off SQL log
2. rsau/SQL-Audit/filename – Pattern of file names
3. rsau/SQL-Audit/logdir – Directory of the file location
4. rsau/SQL-Audit/filesize – Maximum log file size[18]

6. System trace- ST01 transaction is the option to check the internal SAP system activities. System trace can be used to monitor authorization checks, kernel functions, kernel modules, database access, table buffers, lock operations and RFC calls. Database access, table buffers, RFC calls and lock operations can be monitored using ST05 transaction. As shown in the below figure there are multiple components that can be included while conducting a trace for the system [17].

7. Developer trace- Developer trace contains technical information and it can be helpful in diagnosis of the host SAP systems which could prove crucial in forensics analysis of ERP systems. These traces are written in files of work directory in SAP application server that generated the trace. Trace files like dispatcher (dev_disp), message server (dev_ms), RFC, SAP web dispatcher (dev_wdisp), transport programs (dev_tp), internet communication manager (dev_icm) etc. are available in developer traces of SAP ERP systems [19].

3.3 Evidence Preservation

Preserve the integrity of original evidence is the thumb rule in any forensics investigation. Discovery of electronic evidence has different challenges than that of other tangible evidences. Thus it requires special skills to preserve such electronic evidences without tampering the same. Spoliation of evidence can occur knowingly or unknowingly during the incident response proceedings. There are four ways through which evidence can get tampered [10].

1. **Inadvertent spoliation**
   Human errors happen all the time, deletion of SAP ERP systems logs before archiving the same or accidental deletion of data can happen from system administrators or investigators.
2. **Deliberate software spoliation**
   Deliberate deletion or logs or data files can be possible to delete the trace of fraudulent activities in the SAP ERP systems.

3. **Hardware spoliation**
   Hardware spoliation of SAP ERP systems is not that common as physical exploitation of SAP ERP servers is not an easy task.
4. **Date alteration**
   Date changes are makes an impact during case proceedings and tampering date change data in databases can affect the pace of the investigation and it can disturb the investigation links [10].

Preserving the integrity of original evidence is of the topmost priority in forensic investigation, Hash codes are used to preserve the integrity of original evidence. MD5 and SHA1 are the hashing algorithms that are mostly used during forensic investigation. Forensics tools like Encase and FTK computes hash every time the image is opened and closed thus it ensures and verifies investigators and technicians have not changed the image [10].

3.4 Planning the incident response

As it has been identified that system has been compromised, initial assessment of that infected system is critical step in forensics investigation it can also determine whether it's an actual incidence or false positive.

1. **Communicating the incident**- Communications of the incident to higher authorities is important as it will decide the next course of action.
2. **Containing the damage and minimizing the risk**- If some fraudulent activity has happened in any business process of SAP ERP system then initial assessment of authorization loopholes then it can be restricted to prevent the further financial loss to the organization.
3. **Identifying the type and severity of the compromise**- It will decide the nature and scope of resources that are required to address the situation of incident. Point of origin of compromise needs to be identified.
4. **Protecting evidence**- Logs of SAP ERP systems needs to be protected during incident response and will need to make sure that no one alters the critical log information in the system.
5. **Notifying external agencies**- Notifying external agencies is subjective call as most of the organizations are reluctant to notify incidents to law enforcements as it may leak unnecessary information for the competitors or company reputation may be damaged.
6. **Recovering systems**- Recovering or restoring the SAP ERP systems is critical task during incident response as the system is also critical from business perspective of an organization.
7. **Assessing incident damage and cost**- Assessment of incident damage cost is incident response leader's responsibility and it is important for the companies if major loss has occurred.
8. **Reviewing the response and updating policies**- Review of response and policy update is a good strategy so that plan can be assessed to address the situation in a better way [27].

3.5 Data mining forensics evidence

"Data mining of forensics evidence is the extraction of computer crime related data to determine crime patterns."[28] SAP ERP systems contain huge data thus it's a big challenge for law enforcement and forensics investigators to analyze the data involving crime or fraudulent activities. Crime or fraud data mining is classified as entity extraction, clustering techniques, deviation detection and association [28].

1. **Entity Extraction** – It is used to extract user ID, password, system IP and personal properties from logs.
2. **Clustering techniques** – It is used to associate person, organization or systems in crime or fraudulent activity.
3. **Deviation detection** – It deals with tracing abnormal activities in the system for the fraud detection.
4. **Association** – It is used to find the association between the transactions [28].

If an attacker attempts to login in the database and if the associated logs show that data has been deleted or data loss then the motive of attack may be data theft. If the attacker accesses the OS files then motive of the attack may be system crash. If the attacker performs financial transaction by escalating privileges in the SAP ERP system then it can be for fraudulent financial transactions [28].

Streamlined data mining approach can help the administrators in identifying and alerting administrators about similar future attacks. With the data mining techniques SQL injection attacks, brute force attacks, fraud detection can be analyzed efficiently which can save the time and prevent the future incidents [28].

As SAP ERP is specialized ERP product of SAP hence fraud detection on such systems can be managed better with other SAP products like SAP GRC and SAP Fraud management.

4. SAP FRAUD MANAGEMENT

More than 50% of fraud cases are detected by accident after the incident has occurred. It requires lot of costly tools for fraud analysts and it could also return false positives. Thus for effective fraud management we need an approach that can detect the fraud and prevents as it happens. If any fraudulent activity happens then fraud analysts should investigate efficiently and without affecting the business operations of an organization. It can also involve investigation suspicious transactions to achieve compliance to protect company's assets. SAP fraud management can give holistic solution to detect, prevent and deter the fraud [20].

Early detection of fraud can help in preventing the further loss, SAP GRC and SAP fraud management can help to capture and analyze fraudulent activities in ERP systems. SAP fraud management can handle the scenarios like employee theft, corruption and warranty fraud etc. SAP fraud management uses real time calibration and simulation features which improves fraud detection accuracy and avoids false positives. The false positives are reduced by using granular criteria like customizable weighting factors and thresholds which adjusts detection strategies and search rules [20].

SAP fraud management can also help in stopping the transactions that seems fraudulent, it can automatically hold payments if it exceeds the threshold. SAP fraud management can also be integrated with SAP predictive analysis which can help in optimizing the quality of investigation. Thus with this approach fraud analysts can effectively deter the fraud and make better decisions in order to reduce the risk. SAP fraud management can also be integrated with SAP GRC process control which can help in securing the business processes of an organization in effective manner [20].

Fraud management with SAP predictive analysis can perform data modelling and scenario planning which will result in information that can be put forward to decision makers that deals with fraud attack. In memory computing features puts the faster results for real time fraud detection and prevention [20].

SAP defines fraud management as follows, "SAP Fraud Management works with replicated business data to detect, investigate, and help in the prevention of fraud and the assurance of anti-corruption compliance and risk avoidance. Business data can be purchase orders, or insurance claims. Data is replicated from an operational system (source system), such as SAP ERP, and is then analyzed with detection strategies and detection methods. Potential fraud, address-screening hits, and other irregularities can then be detected and reported in the form of alerts, which are then the basis for investigations. Detection performance can be calibrated by what-if-analysis. The process and the results can be integrated into the main business processes and monitored (analysis of detection and investigation). [21]."

SAP fraud management is included in the SAP assurance and compliance software along with SAP business partner screening and SAP audit management. This software is based on SAP HANA platform [21].

User management for the SAP fraud management uses the mechanisms provided with SAP NetWeaver and SAP HANA. SAP Fraud management has two user types. One is individual users and another is technical users, Individual users are dialog users which have profiles like business analyst, fraud investigator and fraud manager. Technical users are RFC users and background users, RFC users are used to communicate with SAP ERP systems and background users are used for processes, like data loading and data extraction [22].

SAP Fraud management standard roles:

1. **SAP Fraud Management: Business Analyst**

SAP_FRA_BUSINESS_ANALYST

This role allows the user to create, maintain and calibrate detection strategies which are based on SQL script procedures. It also allows run the mass detection and also allows to create procedures for detection methods [22].

2. **SAP Fraud Management: Fraud Investigator**

SAP_FRA_FRAUD_INVESTIGATOR

This role allows user to display methods which are based on SQL script procedures. It will also allow the user to create manual alerts, investigate the alerts and close the alerts with decision setting [22].

3. **SAP Fraud Management: Fraud Dispatcher**

SAP_FRA_FRAUD_DISPATCHER

This will allow the user to manage the task list, assign the alerts to fraud investigators, display the detection strategies and methods, investigate the alerts and close them [31].

4. **SAP Fraud Management: Fraud Manager**

SAP_FRA_FRAUD_MANAGER

This role allows the user to monitor the department activities, create manual alerts and close the alerts with decision, maintain high risk countries, maintain suspicious terms, create detection methods, create detection strategies, calibrate detection strategies, display strategy optimization log, running the mass detection and maintaining detection runs [22].

5. **SAP Fraud Management: System Administrator**

SAP_FRA_SYSTEM_ADMIN

This role allows the user to check the technical configuration, display mass detection alerts, delete simulation data, delete incomplete mass detection runs, display optimization log to clean-up the entries, delete alerts, delete detection strategies, delete personal settings, delete calibration simulation and optimization results [22].

6. **SAP Fraud Management: Chief Risk Officer**

SAP_FRA_CHIEF_RISK_OFFICER

This role allows the user to create the alerts manually, maintain tasks, close alerts by setting decision, display detection strategies and calibrate detection, strategy optimization log [22].

7. **Business Partner Master Data screening: System Communication**

SAP_BPCM_SYS_COM

It allows user to call the SAP fraud management via external interface to perform online address screening and create or update the BPMS objects [22].

These are the roles with which fraud management duties can be segregated in SAP fraud management platform of an organization. SAP Fraud management gives real time visibility into business processes and business transactions in an organization.

5. CONCLUSION

SAP ERP forensics analysis requires making the full utilization of technical features provided by SAP platform during the implementation. SAP ERP systems give comprehensive logs of all the system functions which will be helpful during the investigation on SAP ERP systems. The logs include users and authorizations logs, security audit logs, table change logs, change documents, SQL audit, system trace, developer trace.

SAP fraud management gives holistic solution to detect, prevent and deter the fraud. It can help the organization in early detection of fraud which can help in preventing the further loss. SAP fraud management handles the scenarios like employee theft, corruption and warranty fraud by using real time calibration and simulation features which improves fraud detection accuracy and also avoids false positives. SAP Fraud management in integration with SAP predictive analysis performs data modelling and scenario planning which will result in information that is required to deal with fraud attack. SAP ERP systems needs to be ready for forensic Analysis and the applications like SAP Fraud Management, SAP GRC and SAP predictive analysis can help tremendously in SAP ERP system forensics.

REFERENCES

[1]. Boeder, Jochen, and Bernhard Groene. *The Architecture of SAP ERP*. Hamburg: tredition, 2014. ISBN 9783849576622.

[2]. Chastukhin, Dmitry, and Evgeny Neyolov. 'Erpscan's Pentesting Director Talks About SAP Forensics At Confidence'. *Erpscan*. Last modified 2013. Accessed November 13, 2015. http://erpscan.com/press-center/blog/erpscans-pentesting-director-talks-about-sap-forensics-at-confidence/.

[3]. Coresecurity.com,. 'SAP Netweaver Dispatcher Multiple Vulnerabilities | CORE Security'. Last modified 2015. Accessed November 18, 2015. http://www.coresecurity.com/content/sap-netweaver-dispatcher-multiple-vulnerabilities.

[4]. Coresecurity.com,. 'SAP Router Password Timing Attack | CORE Security'. Last modified 2015. Accessed November 18, 2015. http://www.coresecurity.com/advisories/sap-router-password-timing-attack.13. https://www.virtualforge.com/en/blog/post/native-sql-injection-risks-en.html

[5]. Cyberlaw, Consulting. 'Cyber Law Consulting : Cyber Law | Cyber Forensics | Audit And Compliance |Trade Mark And Copy Right'. *Cyberlawconsulting.Com*. Last modified 2015. Accessed November 11, 2015. http://www.cyberlawconsulting.com/erp-audit.html.

[6]. Cyberlaw, Consulting. 'Cyber Law Consulting :Cyber Law | Cyber Forensics | Audit And Compliance |Trade Mark And Copy Right'. *Cyberlawconsulting.Com*. Last modified 2015. Accessed November 11, 2015. http://www.cyberlawconsulting.com/forensics.html.

[7]. Ertunga, Arsal. *SAP Security: Real-life Attacks to Business Processes*. Hack in Paris. Accessed November 28, 2015. https://www.hackinparis.com/sites/hackinparis.com/files/arsal_ertunga_sap.pdf

[8]. Global, Digital Forensics. 'Database Forensics And Database Ediscovery'. *Computer Forensics | Ediscovery | Cyber Incident Response | Cyber Security | Computer Forensics Experts*. Last modified 2012. Accessed November 15, 2015. https://evestigate.com/database-forensics-database-ediscovery/.

[9]. Gutesman, Ezequiel. 'Unprotected SAP Gateways - Evil-Twin And Code Execution Attacks Through Registered RFC Servers | Onapsis'. *Onapsis.Com*. Last modified 2015. Accessed November 17, 2015. https://www.onapsis.com/blog/unprotected-sap-gateways-evil-twin-and-code-execution-attacks-through-registered-rfc-servers.

[10]. Hassell, Johnette, and Susan Steen. 'Preserving And Protecting Computer Evidence'. *Electronicevidenceretrieval.Com*. Last modified 2015. Accessed December 8, 2015. http://www.electronicevidenceretrieval.com/preserving_protecting_evidence.htm.

[11]. Infosecurity Magazine,. 'Anonymous Hacks Greek Ministry Of Finance'. Last modified 2012. Accessed November 18, 2015. http://www.infosecurity-magazine.com/news/anonymous-hacks-greek-ministry-of-finance/.

[12]. InfoSec Resources,. 'The Cyber Exploitation Life Cycle - Infosec Resources'. Last modified 2013. Accessed December 1, 2015. http://resources.infosecinstitute.com/the-cyber-exploitation-life-cycle/.

[13]. Maenkova, Darya. *Chinese attack on USIS using SAP vulnerability*. Seclists.org. Accessed November 27, 2015. http://seclists.org/fulldisclosure/2015/May/64

[14]. Nunez, Mariano. *Cyber-attacks and SAP Systems*. Black hat Europe 2012 briefings. Accessed December 3, 2015. https://media.blackhat.com/bh-eu-12/DiCroce/bh-eu-12-DiCroce-CyberAttacks_to_SAP_systems-WP.pdf

[15]. Official, SAP. 'The Security Audit Log - Auditing And Logging - SAP Library'. *Help.Sap.Com*. Last modified 2015. Accessed December 5, 2015. https://help.sap.com/saphelp_nw70ehp2/helpdata/en/c7/69bcb7f36611d3a6510000e835363f/content.htm.

[16]. Official, SAP. 'Logging Changes Made To User And Authorization Information - Auditing And Logging - SAP Library'. *Help.Sap.Com*. Last modified 2015. Accessed December 7, 2015. https://help.sap.com/saphelp_nw70ehp2/helpdata/en/c7/69bcd8f36611d3a6510000e835363f/content.htm.

[17]. Official, SAP. 'System Trace - Tools For Monitoring The System - SAP Library'. Help.Sap.Com. Last modified 2015. Accessed December 6, 2015. https://help.sap.com/saphelp_nw70/helpdata/en/1f/83114c4bc511d189750000e8322d00/content.htm.

[18]. Official, SAP. 'SQL Audit - Release Notes 45B - SAP Library'. Help.Sap.Com. Last modified 2015. Accessed December 8, 2015. http://help.sap.com/saphelp_46c/helpdata/en/36/b80e890ac039c2e10000009b38f984/content.htm.

[19]. Official, SAP. 'SAP Security Optimization Services | SAP Support Portal'. *Support.Sap.Com*. Last modified 2015. Accessed November 16, 2015. https://support.sap.com/support-programs-services/services/security-optimization-services.html#tabSelector#0_2.

[20]. Official, SAP. *Detect, Prevent and Deter fraud In Big Data Environments*. Ebook. 1st ed. SAP, 2015. Accessed December 7, 2015. http://www.sap.com/bin/sapcom/de_de/downloadasset.2013-09-sep-17-10.detect-prevent-and-deter-fraud-in-big-data-environments-pdf.html.

[21]. Official, SAP. *SAP Assurance and Compliance Software*. Ebook. 1st ed. SAP, 2015. Accessed December 8, 2015.

http://help.sap.com/saphelp_fra110/helpdata/en/65/f38852c7a69f11e10000000a441470/frameset.htm.

[22]. Official, SAP. *SAP Assurance and Compliance Software*. Ebook. 2nd ed. SAP, 2015. Accessed December 8, 2015. http://help.sap.com/saphelp_fra110/helpdata/en/65/f38852c7a69f11e10000000a441470/frameset.htm.

[23]. Onapsis SAP Security In Depth Webcast Detecting White Collar Cyber Crime With SAP Forensics. Video. http://softwareengi.com/computer_crime_and_security/Onapsis_SAP_Security_In_Depth_Webcast_De/464955/: Onapsis, 2015.

[24]. Pctools.com,. 'What Is Zero-Day Vulnerability? | Security News'. Last modified 2015. Accessed November 19, 2015. http://www.pctools.com/security-news/zero-day-vulnerability/.

[25]. Rapid7.com,. 'SAP Web GUI Login Brute Forcer | Rapid7'. Last modified 2015. Accessed November 23, 2015. http://www.rapid7.com/db/modules/auxiliary/scanner/sap/sap_web_gui_brute_login.

[26]. Rashid, Fahmida. *Majority of SAP Attacks Use One of Three Common Technique.* Security week. Accessed November 29, 2015. http://www.securityweek.com/majority-sap-attacks-use-one-three-common-techniques

[27]. Shimonski, Robert. 'Make An Incident Response Plan'. Windowsecurity.Com. Last modified 2003. Accessed December 10, 2015. http://www.windowsecurity.com/articles-tutorials/misc_network_security/Make_an_Incident_Response_Plan.html.

[28]. Sindhu, KK, and BB Meshram. 'Digital Forensics and Cyber Crime Data Mining'. *Journal of Information Security* 3 (2012): 196-201. Accessed December 7, 2015.

[29]. Valenzuela, Ismael. My ERP Got Hacked. Ebook. 1st ed. HAKIN9, 2009. Accessed December 3, 2015. http://blog.ismaelvalenzuela.com/wp-content/uploads/2009/11/my_erp_got_hacked_1.pdf

[30]. Wiegenstein, Andreas. 'Native SQL Injection Risks In SAP'. *Virtualforge.Com*. Last modified 2015. Accessed December 5, 2015. https://www.virtualforge.com/en/blog/post/native-sql-injection-risks-en.html.

[31]. Zysman, Alan. 'Litigation Support & Forensic Accounting'. *Forensicaccounting.Com*. Last modified 2015. Accessed November 12, 2015. http://www.forensicaccounting.com/one.htm.