ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Digital Forensic System Using Web-Application Security for Prevention of Network Attack

Vidyashree M [1], Minavathi [2]

M.Tech Scholar, Dept. of CSE, PESCE, Mandya, Karnataka, India[1]

Professor, Dept. of CSE, PESCE, Mandya, Karnataka, India[2]

ABSTRACT: As of today almost everyone are using internet which has changed the world. As there is increase in the usage and development of it at the same time the security issues are concerned. This paper describes the development of Digital forensic System which helps admin to can track the details of the users who have logged in to the application. Admin can track the IP of users and if they Login from different IP address three times then their account will be blocked. With the emergence and popularity of web application, threats related to web applications has increased to large extent. Among many other web applications threats Structured Query Language Injection Attack (SQLIA) is the dominant in its use due to its ability to access the data. We have also demonstrated a DDoS attack on the server by the hacker due to which the application will be terminated. Many other solutions are proposed in this regard that has success in specific conditions and helps to detect the SQL injection.

KEYWORDS: Structured Query Language Injection, distributed denial-of-service (DDoS), Digital forensic System

I. INTRODUCTION

Web applications are major source of information for business process critical for the survival for any organizations. With the popularity of web applications there is also increase in web application vulnerabilities. Across many types of web vulnerabilities SQL Injection (SQLI) has become the predominant method due to its rewarding nature to have access to the data and due to advances in its techniques. It is observed that SQL injection is the most widely used techniques for the web applications. Due to huge rewarding of having access to the database the SQLI has become the predominant web application security risks and their technique has become more sophisticated over time. Due to emergence of different sophisticated techniques SQLIA has shown a tremendous increase in its spread to web applications of finance banks, educational institutes, global market and many more. SQLIA is also among the top when compare the spread or choice of web vulnerability among the intruders. For smooth operations of the organization that utilize web applications it is necessary that web applications operate at reasonable level of security. Due to complexities of web technologies and varieties of risks it is not an easy task to save the web applications from intruders and threats. Even sometimes it is very difficult to detect that some serious threat has been occurred. A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination. Figure 1 describes the overview of digital forensic analysis system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

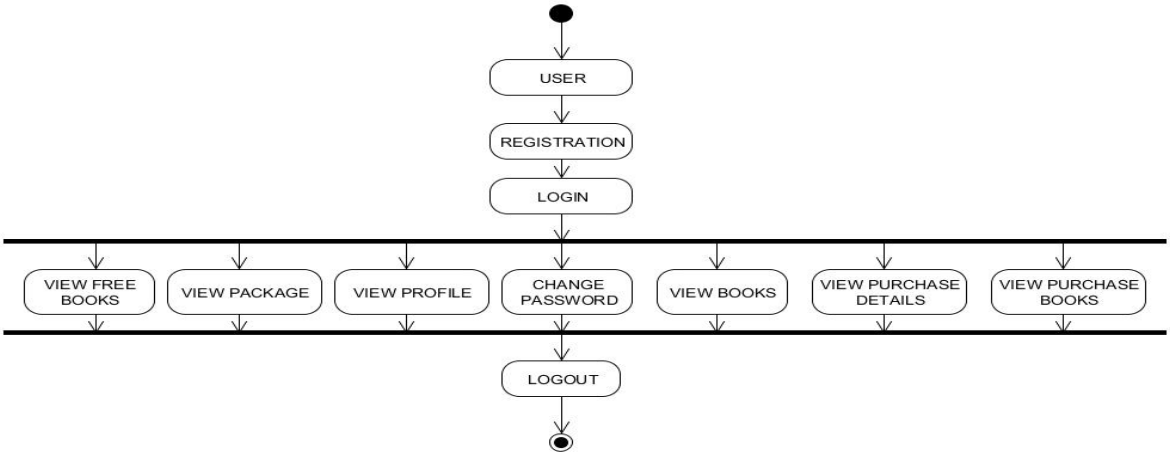

Fig 1: Overview of digital forensic analysis system

Penetration of Internet users in 1995 only 1 percent of the world population and in 2014 the figure had reached 40 percent or 3 billion users, 1 billion websites and the increasing. Alarming number of Cyber attacks to a target individual that continues to grow each year. Heightened attacks and Cybercrime have finally been made a loss in the business sector, government, communities and individual targets that caused the issue becomes serious attention from Governments, corporations, and the research community.

These are the steps for conducting computer forensics investigations:

- Policy and Procedure Development.
- Evidence Assessment.
- Evidence Acquisition.
- Evidence Examination.
- Documenting and Reporting.
- Digital Forensic has been implemented in detection of crimes going on networks and it stores the evidence from which the crimes can be exposed easily. It is also used in private investigation.
- Session hijacking is predicted by using the different types of forensics.
- Simulation of single victim attack has been identified where the person by knowing the email id can attack the victim which can be prevented using forensics.
- Digital forensics is the application of scientific principles to the process of discovering information from a digital device. A form of digital forensics has been around nearly as early as computers were invented, but forensic capabilities have witnessed many advances in the past years as digital forensic processes have matured and needs have become more prevalent. Digital forensics can involve nearly any digital device, not just computers, although technology often evolves faster than forensic capabilities do. Some of the common areas in which digital forensics is used include computers, printers, cell phones, mobile devices, global positioning systems (GPSs), and storage media. Less common areas include automobile systems, appliances, office equipment, and other programmable devices.

This paper is organized in to five sections. Brief introduction about digital forensic system and its need is discussed in section I. A brief literature survey, involving the contributions of various researchers in this field, is discussed in Section II. Section III tells more about the proposed digital forensic system to prevent network attack. After this section,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

the section 4 described the experimental results and finally, the conclusion and scope for future work is discussed in section V followed by the references.

II. RELATED WORKS

To date, little attention has been paid to SQL injection attacks. Many approaches have been proposed for preventing SQL injection attacks. Runtime approaches are useful for protecting deployed software, but static approaches are desirable during software development and testing for a number of reasons. Although the security vulnerability has persisted for some time, recent efforts by hackers to automate the discovery of susceptible sites have given rise to increased invention by the research community as discussed in this section.

Xiaoyu Du et al [1], aims to evaluate the applicability of existing digital forensic process models and analyse how each of these might apply to a cloud based evidence processing paradigm. Digital forensic science is very much still in its infancy, but is becoming increasingly invaluable to investigators. A popular area for research is seeking a standard methodology to make the digital forensic process accurate, robust, and efficient. The first digital forensic process model proposed contains four steps: Acquisition, Identification, Evaluation and Admission. Since then, numerous process models have been proposed to explain the steps of identifying, acquiring, analyzing, storage, and reporting on the evidence obtained from various digital devices. These models attempt to speed up the entire investigative process or solve various of problems commonly encountered in the forensic investigation. In the last decade, cloud computing has emerged as a disruptive technological concept, and most leading enterprises such as IBM, Amazon, Google, and Microsoft have set up their own cloud-based services. In the field of digital forensic investigation, moving to a cloud-based evidence processing model would be extremely beneficial and preliminary attempts have been made in its implementation. Moving towards a Digital Forensics as a Service model would not only expedite the investigative process, but can also result in significant cost savings – freeing up digital forensic experts and law enforcement personnel to progress their caseload.

Irma resendez et al [2], described a complete overview of digital forensics. As new technologies develop criminals find ways to apply these technologies to commit crimes. With the explosion of web technologies almost all major businesses in the world have web presence thus exposing their data to legitimate and illegitimate users. Computers have become intrinsic part of our lives. Businesses have streamlined their operation saving millions of dollars because of the web technologies and services. Neither the businesses nor the consumers can live without these technologies. Because of the intricate involvement of computer technology in all aspects of our lives, it also has become legal evidence in both civil and criminal cases. Computer evidences admitted in courts could be any file or fragment recovered from the storage devices such as email, browsing history, graphics, photographs, or application documents. These files may be undeleted or deleted. Deleted file recovery would require special techniques. Computer professionals trained in digital forensics preserve and retrieve evidence in a non-destructive manner. Evidence may be recovered from any storage medium installed in digital equipment such as computers, cameras, PDAs, or cell phones. All forensic work should be done with care including documenting clear chain of custody in order for the evidence to be admissive in a court of law.

Bojan Jovičić et al. [3], focused on attacks against Web applications, either to gain direct benefit by collecting private information or to disable target sites. Web applications security is one of the most daunting tasks today, because of security shift from lower levels of ISO OSI model to application level, and because of current situation in IT environment. ASP.NET offers powerful mechanisms to render these attacks futile, but it requires some knowledge of implementing Web application security. It describes the two most common Web application attacks: SQL Injection and Cross Site Scripting, and is based on author's perennial experience in Web application security. It explains how to use ASP.NET to provide Web applications security. There are some principles of strong Web application security which make up the part of defense mechanisms presented: executing with least privileged account, securing sensitive data (connection string) and proper exception handling (where the new approach is presented using ASP.NET mechanisms for centralized exception logging and presentation). These principles help raise the bar that attacker has to cross and consequently contribute to better security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Rutvi Pradipkumar Adhyaru et al. [4] have introduced all web application based attack including two major attacks like XSS (Cross Site Scripting) and SQLI. The web is absolutely necessary part of our lives. It is wide platform which is used for information sharing and service over internet. They are used for the financial, government, healthcare, education and many critical services. Everyday billions of user purchase items, transfer money, retrieve information and communicate over web with each other. Although the web is best friend of users because it provide anytime anywhere access to information and services at the same time. All things are created by human in the world so its reality that the things created by man are little bit problematic. So web applications are also created by human so it contains too many loopholes. The popularity of applications allures hackers towards them. Now a Days Securing and maintaining the websites against attack is very hard and challenging task. Finding loopholes in Web application, Computer system or network and exploiting them called hacking. New approaches for web attacks are invented day to day so the study of detect and prevent against web application attack and finding solution is important part in internet world.

R. K. Deka et al.[5], discussed several prominent approaches introduced to counter DDoS attacks in private clouds and also discussed issues and challenges to mitigate DDoS attacks in private clouds. They have highlighted issues and challenges faced in the private cloud environment when providing defense solutions against DDoS attacks. Some useful approaches developed by researchers to address these issues have been presented and analyzed. The importance of mitigating the attack by tolerating it and by optimized use of resources in the private cloud scenario has been emphasized. Finally, the role of big data analytics in defending DDoS attacks in the cloud has been introduced. In the near future, authors have planned to deploy the conceptual cloud framework in a testbed to demonstrate and analyze the effectiveness of our proposed solutions. The future of the Internet is predicted to be on the cloud, resulting in more complex and more intensive computing, but possibly also a more insecure digital world. The presence of a large amount of resources organized densely is a key factor in attracting DDoS attacks. Such attacks are arguably more dangerous in private individual clouds with limited resources.

III.PROPOSED SYSTEM FRAMEWORK

In Proposed work, if admin login by providing username and password or attacker login by using SQL injection in admin login page, those credentials of the device sent to the admin email ID in both the cases. Here, the hacker also makes a DDoS attack on the webpage of the user by running the script which has the port number of the particular website because of which the entire working of the application will be stopped this can be overcome by the users by running the same script with the port number of hackers website.
In the existing system there is no efficient and advanced system for detecting the vulnerabilities in the web. It has been observed that due to access to the data base SQLIA has become the dominant web application security risks over the last ten years. Database is the very critical for successful operations of any organization. Sensitive information in the database can be used in many ways to serve the attacker purpose. So it is not efficient and fast, not reliable and secure and time consuming process.

Methodologies followed in proposed system are creating an example web application, uploading and launching application, then try to attack the uploaded server using SQL injection technique, analyze the type of attack and find a prevention solution for it, at last resolve the attack. A use case diagram present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases is shown in figure 2.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

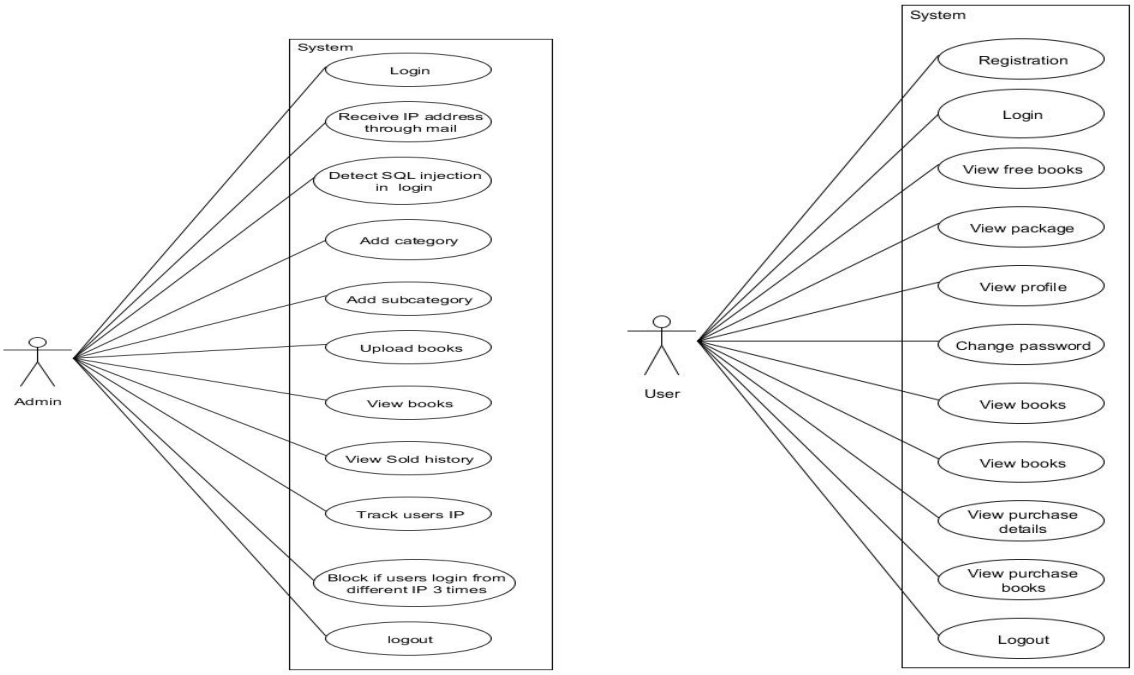

Fig 2: Use case diagram of the digital forensic analysis system to prevent network attack

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart shown in figure 3.

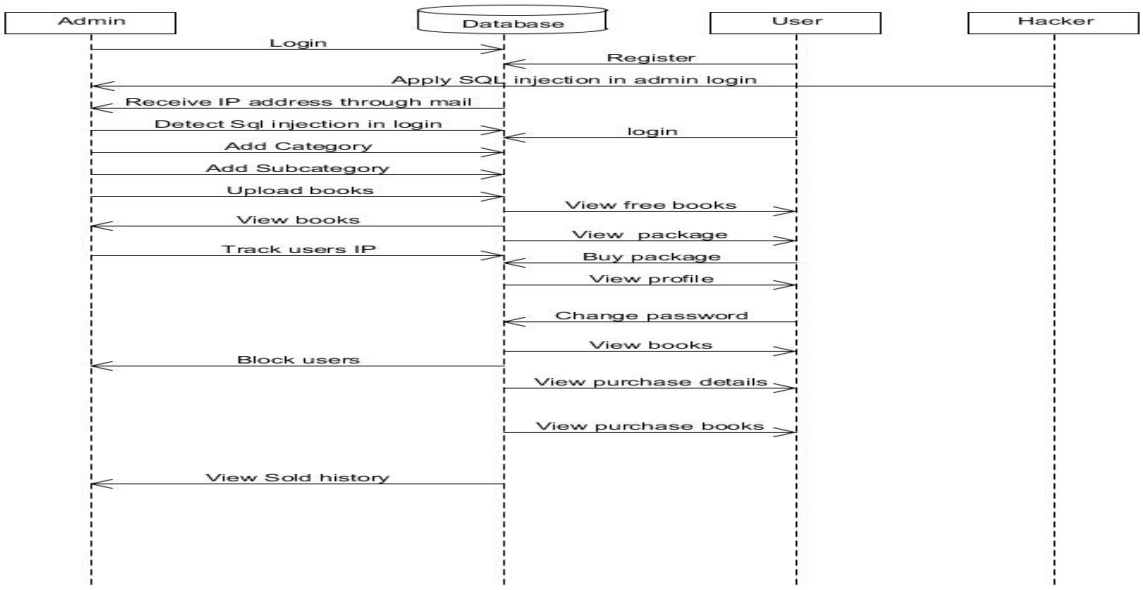

Fig 3: Data flow diagram of the system the digital forensic analysis system to prevent network attack

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

IV. EXPERIMENTAL RESULTS

The proposed digital forensic analysis system to prevent network attack using web application security is implemented using windows7/8/10 on tomcat 7.0 server, Core i3/i4 CPU @ 2.1GHz, 25 GB RAM followed by scripts using JDBC database connectivity. The results are tabulated in Table 1 is represented below.

Table 1: Validation results of the digital forensic system to prevent network attack

Test case ID	Test case name	Test case description	Test steps				Test status P/F
			Step	I/p given	Expected o/p	Actual o/p	
TC01	Login	To verify that the User has entered Valid username and password	Login with Username & pswd	Valid Usn & Pswd	Login successful	Login successful	Pass
	Login	To verify that the User has entered Valid username and password	Login with Username & pswd	Invalid Usn & Pswd	Login successful	Error Enter valid Usn & pswd	Fail
TC02	Registration	To verify that the user has registered by entering valid details	Enter all the valid user details	Valid details	Registered successfully	Registered successfully	Pass
	Registration	To verify that the user has registered by entering valid details	Enter all the valid user details	Invalid details	Registered successfully	Not Registered successfully	Fail

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

V. CONCLUSION AND FUTURE ENHANCEMENT

The Digital forensic application is designed to provide the basic detection techniques of web application attacks so as to secure the systems present in the networks that are directly or indirectly connected to the Internet. Performing such a duty always goes in hand on hand diving success as well as failure in fulfilling the objective. But finally at the end of the day it is up to the Network Administrator to make sure that his network is out of danger. The developed application does not completely shield network from Intruders, but helps the Network Administrator to track down hackers on the Internet whose very purpose is to bring your network to a breach point and make it vulnerable to attacks.

In the future, it can be extended by incorporating Intelligence into it in order to gain knowledge by itself by analyzing the growing traffic and learning new attack patterns. The present system runs on an individual host machine and is not a distributed application. This can be extended to make it a distributed application where different modules of the same system running on different machines may interact with each other thus providing distributed detection and protection for all those machines on which the system is running.

REFERENCES

1. Du, Xiaoyu, Nhien-An Le-Khac, and Mark Scanlon. "Evaluation of digital forensic process models with respect to digital forensics as a service." arXiv preprint arXiv:1708.01730(2017).
2. Resendez, Irma, Pablo Martinez, and John Abraham. "An introduction to digital forensics." (2012).
3. Jovičić, Bojan, and Dejan Simić. "Common web application attack types and security using ASP .NET." ComSIS. December (2006).
4. Adhyaru, Rutvi Pradipkumar. "Techniques for attacking web application security." International Journal of Information 6, no. 1/2 (2016).
5. Deka, Rup Kumar, Dhruba Kumar Bhattacharyya, and Jugal Kumar Kalita. "DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment." arXiv preprint arXiv:1710.08628 (2017).
6. William Stallings, "Cryptography and Network Security", Principles and Practices, Third Edition.
7. D. E. Denning, "An intrusion-detection model". IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987.
8. Stephen Northcutt, Judy Novak, "Network Intrusion Detection", Third Edition, Pearson Education 2003.
9. Kieyzun, P. J. Guo and K. Jayaraman, "Ernst. Automatic creation of sql injection and cross-site scripting attacks," in 31st International Conference on Software Engineering, ICSE ˝09,, Washington, 2009.
10. Liu, Y. Yuan, D. Wijesekera and A. Stavrou, "Sqlprob: a proxybased architecture towards preventing sql injection attacks," in 2009 ACM symposium on Applied Computing, SAC ˝09, New York, 2009.
11. S. Gordeychik, 15 December 2013. [Online]. [Accessed December 2013].
12. Razzaq, A. Hur, N. Haider and F. Ahmad, "Multi-layered defense against web application attacks," in Sixth International Conference on Information Technology: New Generations, Washington, DC, 2009.
13. Tajpour, M. Massrum and M. Heydari, "Comparison of sql injection detection and prevention techniques," in Education Technology and Computer (ICETC), 2010 2nd International Conference, 2010.
14. D. A. Anup Shakya, "A Taxonomy of SQL Injection Defense Techniques," Karlskrona Sweden, 2011.
15. Tajpour and .. Shooshtari, "Evaluation of sql injection detection and prevention techniques," in Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference, 2010.
16. Gary L Palmer.(2001). A Road Map for Digital Forensic Research. Technical Report
17. Alam, Delwar, Md Alamgir Kabir, Touhid Bhuiyan, and Tanjila Farah. "A case study of sql injection vulnerabilities assessment of. bd domain web applications." In 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), pp. 73-77. IEEE, 2015.
18. D.A. Kindy and A.S. Pathan "A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques," 15th IEEE International Symposium on Consumer Electronics (ISCE, Singapore, pp.468-471, June 16-19, 2011.
19. E. Bertino, A. Kamra, and P.E. James, "Profiling Database Application to Detect SQL Injection Attacks," IEEE Conference on International Performance, Computing, and Communications Conference, (IPCCC 2007), New Orleans, Louisiana, USA, pp.449-458, April, 2007.
20. P. Mittal, A. Kamra, and S.K. Jena, "A fast and secure way to prevent SQL injection attacks," IEEE Conference on Information Communication Technologies (ICT), Tamil Nadu, India, pp.449-458, April, 2013.
21. Tajpour, A. Kamra, and M.J.Z. Shooshtar, "Evaluation of SQL Injection Detection and Prevention Techniques,"Second International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN),Liverpool, United Kingdom, pp.216-221, July, 2010.
22. Al-Mahrouqi, Aadil, Patrick Tobin, Sameh Abdalla, and Tahar Kechadi. "Simulating sql-injection cyber-attacks using GNS3." In The 6th International Conference on Computer Modeling and Simulation (ICCMS 2015), Amsterdam Netherlands, 12-13 February 2015. International Journal of Computer Theory and Engineering, 2015.
23. Lubis, Akhyar, and Andysah Putera Utama Siahaan. "Network Forensic Application in General Cases." IOSR J. Comput. Eng18, no. 6 (2016): 41-44.
24. M. T., B. B., B. T. M., R. Rajaram dan B. V. K., "Network Forensic Investigation of HTTPS Protocol," International Journal of Modern Engineering Research, vol. 3, no. 5, pp. 3096-3106, 2013.