FORENSICS ON A HACKED WEBSITE

T. Lokesh Sai Reddy
M. Tech - 1st Year, Cyber Forensics and Information Security Department of Computer Science,
Gitam Institute of Technology and Management Visakhapatnam

ABSTRACT

These days, web applications are becoming a target for security attackers. By using some security measures we can prevent or detect security attacks on web applications, but we cannot detect the attacker. Since we are unable to trace the attack, it encourages the attackers to launch new attacks on the same system. Forensics on web applications provides security to the founder from the attacks. By this way we can significantly reduce the number of attacks on daily basis.

Keywords: Security, Attacks, Forensics, Web Applications, Cyber Criminals, Hackers, Evidence, Investigation.

INTRODUCTION

With the development of technologies, web applications are becoming the primary means for transmitting information to government agencies, business and individuals. Web applications support many latest network applications such as e-commerce, e-banking, e-mail, e-medicine, etc. Dependencies on web applications also leads to an increase in security attacks. The dependencies include network infrastructure, web servers, data servers, web browsers and the servers where the applications were installed. Web applications create an environment for attackers to carry out security attacks. This includes various methods such as Cross-site Scripting, SQL injection, Code injection and Buffer Overflow. As long as web applications are the source of data communication over the internet, various network applications are designed to protect against security attacks. Firewalls and system security are designed to prevent the web applications from attacks whereas intrusion detection systems and anti-virus are used to detect an attack.

Depending on the attack plan, it is important to build the ability to track and expose the attacks of the cyber criminals. By doing this we can significantly reduce the number of daily attacks. Tracking the security attacks on the web applications is to identify from where the attack has originated from, how they were distributed and who are responsible for these attacks.

To address these attacks web applications forensics creates a new branch called digital forensics to deal with cyber criminals.

Looking back on the security attacks, forensic investigators rely on the fingerprint traces or the digital evidence left behind by the hackers during the crime scene and on the configuration files. The digital evidences to be investigated can be found in web servers and server logs of the web applications.

To effectively implement forensics on web applications we need to come up with a number of strategies that can effectively manage various digital evidence sources. These are considered as forensic tools. These strategies provide an effective analysis of the data. The different forensic tools used are Microsoft Log Parser, Event Log Analyser, HTTP- Analyzer, Analog, Open Web Analytics, Core Wisdom, etc.

Web Application Forensics

The aim of web application forensics is to track and claim security attacks from the founder. Looking back at the security attacks, forensics rely on log files of various web application items (i.e web browser , web server , data servers and application servers) . Web forensics is not concerned about the network level protocols. Scanning the network log files (i.e IP Routers , IP Switches , Access Systems and Firewalls) may help in research of forensics in web applications. A web forensic investigator should carefully look into the support functions of forensic tools to successfully conduct a security attack on web applications.

While digital forensics looks into image manipulation, operating system looks into the analysis of log files with relation to system changes. Like network forensics, operating system forensics and digital forensics go hand in hand and form support for successful submission of web application forensic research. Finally we should be aware that web forensics does not address security attacks on web services. The forensic investigation into web security attacks is covered by Web Service Forensics which is another branch of digital forensics.

Forensic Investigation On A Web Application Security Attack

A successful forensic investigation relies on pre-analysis phase and needs to follow a certain procedure.

A. Preliminary Analysis

The following initial actions are required for successful forensic investigation of security attacks on web applications.

Forensic Application : Web applications should be prepared for forensic research. This can be achieved by:

Evidence Gathering: In preparation of web applications for future research, it is recommended to enable login option to collect large amounts of digital evidence. If the login options are left unattended in settings, then the collection of evidence would be incomplete and
the final report would not be ready for submission.

Evidence Protection: Given that the log files will be the main source of evidence for forensic investigators, it is important to protect these files to prove the authenticity of the data it contains. The following actions can be considered for protecting the log files:

1. Setting appropriate permissions on the log files
2. Keeping the log files inaccessible from hackers.
3. Checking the integrity of the log files.

Support Forensics : Support forensics tools are used to collect the required digital evidence that cannot be provided by web application login. The evidence needed to conduct the forensic investigation about web application security attacks can be provided by network forensic tools of the operating system or by a third party service.

The power of forensic investigator :

1. They should understand the web application (i.e construction , working , target application)
2. They should understand the security issues of the web applications.
3. They should be well trained in using forensic tools.

B. Methodology

It is important to conduct forensic investigation successfully using a standard procedure for web application security attacks .

1. Protect the system during the forensic investigation to prevent any alteration of the data files.
2. Find and gather all the files required for forensic investigation.
3. Perform analysis of the target files to determine the sequence of events. In this step the forensic investigator should classify the log files according to the user’s file time , which gives the investigator a better understanding of the flow of files and the movement created by the users. During the flow session the forensic investigator should be notified of any presence of fingerprints during the attacks.
4. Prepare a report based on the information collected during the investigation.
5. Recommend post event actions.

C. Supporting Forensics

The purpose is to show how network forensics , digital image forensics and operating system forensics can support research on access to web application forensics with the help of more evidence. In fact , the log data that is obtained from the login detection system can accurately help to detect attacker activities. Evidence collected from hacked websites leads to lack of adequate information in the log files.

Web Application Forensic Tools:

Given the amount of logged data that needs to be examined during forensic investigation, automated tools have been suggested for successful deployment of the web application.

Requirements for web application forensic tools

A detailed presentation of the basic forensic tools for web application tools has been presented. The following are the basic requirements for web application forensic tools:

1. Analyze the log files in different formats.
2. Take two separate formatted tested files and assemble them.
3. Manage large log files.
4. Use common expressions and binary concepts as a parameter for the log file.
5. Always consider timestamps while doing investigation.

6. Keep a list of suspicious files and applications that indicate the possibility of revealing important information or clues which may be helpful during investigation.
7. Decode the URL into a readable format which may be useful.

Web Application Forensic Tools

We will have a brief overview of the important forensic tools used, such as Microsoft LogParser , Eventlog Analyzer , HTTP Analyzer , Pyflag , Analog , Open web Analytics , Mywebalyzer.

Microsoft LogParser : This tool was developed by Microsoft , LogParser is a flexible command line application that provides universal query access to text based data such as log files , XML files , W3C files , TSV files and CSV files. Logparser produces output in certified formats such asCSV, TSV, XML, Syslog, W3C, IIS, SQL, and unconventional formats, which require immediate launch or input output such as DATAGRID,CHART and NAT. Logparser does not provide a graphical interface, but offers functionality by requesting a command line with a script, or by direct decryption queries via a fast visual interface. Logparser language includes a set of functions that enable thread decryption, mathematical performance, and provide access to system information.Each of these functions can modify or control the content of the fields in some way. Logparser has the ability to combine data from multiple sources, and query it. Logparser is used to monitor user activity, monitor system file integrity, monitor SQL injection attacks, detect excessive failed login attempts, determine malicious modifications,detect aggressive attacks,and re-enter. As a limitation of this tool, Logparser does not include analytics methods, only the ability to query questions.The user should create useful questions to satisfy any analytical requirements.

EventLog Analyzer : This tool is a real web based log solution and security data management that enhances internal network security. EventLog Analyzer Can Collect,analyze,search,report and archive a wide range of machine generated logs found in Systems (Windows, Linux, UNIX…), network devices (routers, switches, etc.), applications (i -Oracle, Apache, IIS, etc.) and provide important information on network user activity, policy violations, network instability, system downtime, and internal threats. EventLog Analyzer can be used to generate archive files, which can be saved for later analysis. It can also define automated alerts,generate historical styles based on system events, group hosting details together to show interoperability, show failed login, malicious users and show applications causing work or security issues. In addition, EventLog Analyzer incorporates reconstituted reports and allows data selection and the appropriate format for creating custom reports and templates. Reports are periodically released and can be exported in HTML, PDF and CommaSeparated Values (CSV) formats. Analysis can produce both graphs and text-based presentations as output. EventLog Analyzer performs many important features in the forensic log analysis tool. However, it does not include automatic overlap between log files, or extensions regarding non-logged file types.

HTTP Analyzer : Http-analyzer is a log file analyser that can be used to process data in only three log file formats (i.e CLF , ELF and Distilled Log Format(DLF)). The http analysis tool offers the option to create one of two separate HTML reports to include summaries of statistical information and access. These reports include graphs, table data, and three-dimensional forms. Real-time analysis is only available by typing the logs of log files, which are used in conjunction with the default calling of this tool. The Http-analyze forensics tool does not generate or format file login information in any way. It does not enter data into a database, nor does it make connections between web server files with any other available system information.

Pyflag : Pyflag is an open source web application that allows forensic analysis on its log files using Graphical User Interface (GUI). By using this tool we can manage large volumes of log files in multiple formats, disk or images. Data can be added to MySQL database for quick queries but logtypes are still specified by the end user because the basic log function of this tool is to view log files only, the analyst must perform the necessary analysis using prior knowledge and experience. The log data analysis interface includes query, filter and clear display of log data. In addition to the functionality of statistical log analysis, Pyflag offers the option to analyze multiple formats in addition to only log files related to web applications.

Analog : Analog is an open source web file analyst which accepts files of AWS or IISW3C format as an input. As a result analog produces complex graphs and reporting styles when used in combination with another tool called Report Magic. Statistical reporting or the conversion of statistical information into graphic representation enables the basic functioning of this web application forensics tool .Analog generates standard summaries,time-based reports, hosting reports, domain and organization,file-based, browser-based and user and status reports.The validity of the information stored in these reports is maintained only when the required server configuration is performed. Analog requires additional configuration on the part of the analyst to provide a brief account explaining details that will be useful to both marketers and scientific researchers.

Open Web Analytics : The Open Web Analytics platform is a standard web analytics framework that provides analytical data for any application. Due to its nature as a web application, Open Web Analytics can work on any application that contains a browser and can be easily added to existing web applications that use JS, PHP or RESTapplication programming interface. Open Web Analytics provides built-in support for Word press or MediaWiki programs. The main function of the Open Web Analytic tool is to provide real time tracking, monitoring and reporting of web usage statistics. Other examples of informationI can provide include guest click clicks,guest location indexes, browser details and specific web application features. It also provides ways to improve performance by using plugins.

Mywebalizer : Mywebalizer is an open source source for detailed and easy-to-use HTML reports on web server statistics for both tabular and graphical formats. Mywebalizer is completely written in C-language and is highly compatible with various operating systems. It can analyze log files of various formats. In addition to this , Mywebalizer tool provides power compressed capabilities so that compressed files can be directly used without the need of storage space and provides compliance for larger files.

CONCLUSION

Web application forensics is a branch of digital forensics. A right approach is helpful in successfully carrying out forensic investigation in web application security attacks. Network forensics, Digital image forensics and operating system forensics can support forensic research by providing additional evidence.

REFERENCES

1) https://www.acunetix.com/blog/articles/using-logs-to-investigate-a-web-application-attack/
2) http://www.http-analyze.org/
3) https://fr.slideshare.net/test2v/web-application-forensics-taxonomy-and-trends