ISSN:2320-0790

An International Journal of Advanced Computer Technology

An Analytical Study and Synthesis on Web server Security

Jyoti Pandey, Manoj Jain

Abstract: Web servers are being as a viable means to access Internet-based applications. Latest Approaches to secure Web servers are not much efficient or robust enough to protect and their applications from hackers. There are several approaches and analogies to examine the minimum-security requirements of a system. But The Highly efficient Techniques approaches as Protection profile, a systematic approach Therefore, we derive the Web security components that make a secure Web server from the Web Server Protection Profile. Study of A component-based framework as well as an open source solution has been done subsequently in this paper We believe that after the studying of such a system (implemented and deployed later), it will function reliably and effectively. This work aims at establishing the provable reliability of construction and the feasibility of component-based solutions for the secure Web server. This paper gives a theoretical approach and analogy of Profiling a web server including All three basic security models together(System security, Transmission security & Access Control System)etc.

Keywords: Adjustable, Open Source, Protection Profile, Security, Web Server, Web Component, and Network.

I. INTRODUCTION

The internet is an open information system. It is a medium that is always available through a variety of frequently used devices like mobiles, tablets, laptops and so on. Many services havebeen r a p i d l y started making appearances on the web. These include Railway reservation, e-banking services, on- line shopping etc. These services often become house of data and information provided by this data consists of personal data and sensitive information. This has lead to an army of negative minded person who are bent open unethical methods for capturing the data. However developing security methods for the Web is a daunting task, in part because security concerns arose after the fact. We usually considered Web server security apart from Web security. Web servers are essential components in a wide variety of systems, ranging from s i m p l e f i l e sharing to business-critical applications. Given the pervasive nature of web servers, the security attributes of these systems become a very important aspect. Often, these systems are used in contexts where security breaches may cause extensive damage, including financial damage and privacy loss.

II. MOTIVATION & OBJECTIVE

Web security basically consists of three essential components [5]: System Security (server security, host security), Transmission Security (data transportation security, mobile code security) and Access Control (anonymity and privacy). Having all these three elements together being made robust and efficient respectively, the Web server could be treated secure. Their relationships are described in Figure 1.

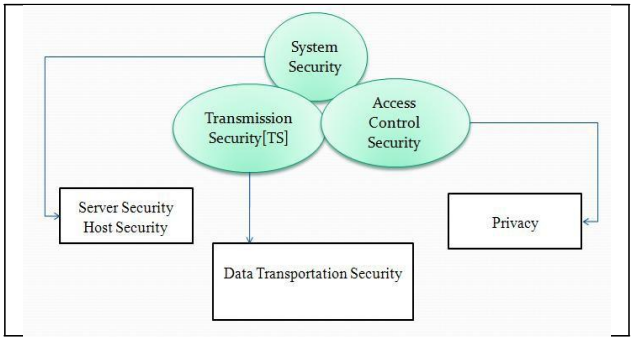


Figure 1: Three Essential Web-Security Components

System security should be carefully considered under each of the circumstances. Experienced/Smart a t t a c k e r s often gather information about a target system to exploit a discovered vulnerability before launching a specific attack. Transmission security addresses authentication, non-repudiation, integrity and confidentiality of the data communication between sender and receiver. Cryptography [3] is an important element of any strategy to cope with those transmission security requirements. Access control deals with the issue on management of

system resources toward system processes and/or users. One of the approaches is to using cookies. Cookies were invented to keep continuity and state on the Web. However, sensitive information cannot be securely stored and communicated in typical cookies.

Besides, most organizations now resort to using firewall to protect themselves from hostile attackers on the Internet. The security policy usually summarizes to total trust of all insiders and total mistrust of outsiders, where the firewall defines boundary. Nevertheless, not all outsiders would be denied. Not all insiders should be trusted either.

From the Web Server Protection Profile provided by various Standards , we can figure out minimum-security requirements for a secured Web server used in open Informative Era, and can propose a framework/closed system for secure Web server possibly by using various tools which motivate us to develop software / Fully secured System / Implemented Methodology for tracing various events of web- server in order to detect any malicious attack on web server which helps in reducing threat of attacks on web-server in real world.

III. BASIC THEORY

Web Server is nothing but a computer Program that dispenses WebPages as they are requested to proceed; The Machine the program runs on is usually called a Server as shown in Fig.2. The Web Server is the program or machine that responds to that request, and delivers the content of the page back to the user.

There is a clear and straight difference between Web security and web server Security, To make a protection profile of both web security and web server security has different discriminations.

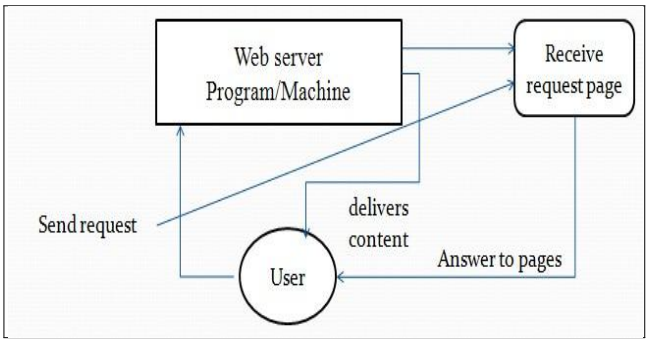


Figure 2: Web Server Operation

Developing security techniques and approaches for a Web itself is a very critical task while in Web server System Security concerns arose after the facts.

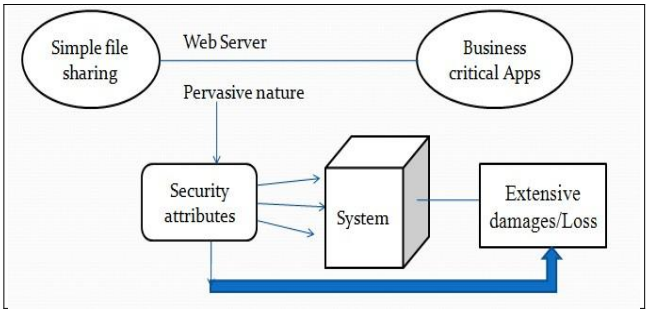


Figure: 3

Mechanisms also constitute the dimensions to taken into account when handling security profiling.

Requirements define the security objectives that a given security methodology must achieve. Policies are statements defining what is and is not allowed in the system. Mechanisms constitute either tools or operational procedures to implement the policies. In fact, security policies are the basis for the development of operational procedures, the establishment of access control rules and various application, system, network, and physical controls and parameters.

Web Server Profiling

For the purpose of complete secured server from any outside threat It becomes necessary to make a profiling of server , The focus of that is to develop methodology that can monitor web server activities taking in to security aspect of web server, There are several commercial tools/ software s which can be used in its profiling[2].

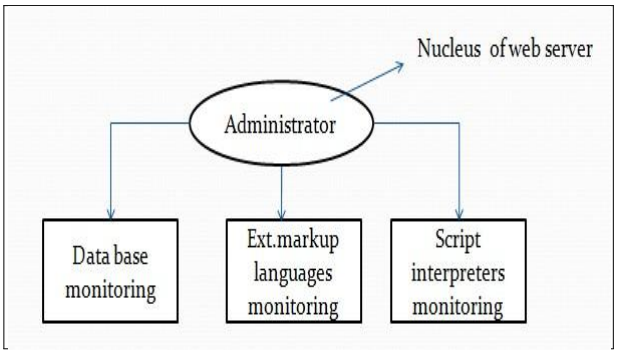


Figure: 4

As shown in figure, administrator of webserver works as Administrator, which helps it in to making a para-series interface so that it can parallel look into its monitoring with a concern of its series security blocks as system, transmission and access control. To considering as a threat in any Web server security system, Any Fault and loop hole in this can lead to loss of Important Personal data as well as sensitive Information.

IV. WHAT EXACTLY SECURITY CONCERN IS ABOUT WS

Security is supposed to existence of three fundamental attributes in any given system: integrity, availability, and confidentiality. Integrity refers to the maintenance of the consistency of the information. Availability means that the system is ready for authorized users. Confidentiality means that only authorized users must access private and very important information. sometimes requirements, policy, and Main objective of the Web Server Protection profile is to monitor web-server activities by taking into consideration monitoring events like TCP/IP connections originated on web- server, security aspect of web-server which deals with file protection and analyzing tracing activity generated by system process and System calls in Linux System.

Major objectives of Web-Server Protection Profile-:

- Securing Web Application Directory.
- Securing TCP-IP Connection.
- Process Monitoring

Web server protection Profiling block diagram is shown as in figure.

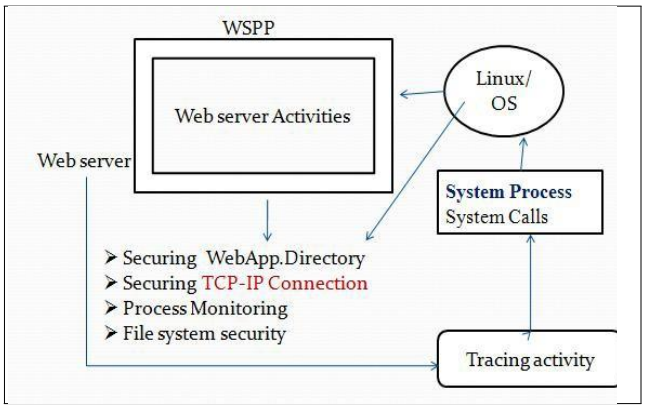


Figure: 5

Any tool supports for the Linux Operating System that allows developers and system administrators to deeply investigate the behavior of the kernel and even user space applications in order to discover error conditions, performance issues, or just to understand how the system works.
The Web Server Protection Profile (PP) is also used to address the security problems of a Web server system, without considering the requirements of the user (who wants to share their data restrictedly) and also ignoring all the security threats that may derive from the connection of the system with other network device. This includes items like denial-of-use attacks, hacker access to the spoof attacks, unauthorized access problems.

After Profiling the WSS, The security assessment[4] is made by performing tests on the target web server that identify which security profiling practices are implemented , The security comparison is made by assessing the security of different web servers in order to identify which web server installation is the most secure.

In Relation with this following steps are preceded:

- Identification, definition and characterization of security practices
- Estimation of the relative importance of security best practices
- Definition of a set of tests to systematically verify if the security best practices proposed are being applied in a given web server installation.

WSP: System Security

System security is evaluated from its functions and administration. Hence we describe our system by means of functional and administrative points of view respectively and deals with direct interface among Server security and Host security.

Functional elements of system security interface The security-adjustable Web server which is commonly proposed for achieving Web components security **has** eleven major functions: kernel, firewall, Web server, **FTP** server, SSL, application firewall, accounting, administration, recovery, exception handling, and configuration.

- ***Kernel*** has the significant influence on system security. It is **also** the key component that accounting and authentication depend upon.
- ***Firewall*** supports data transmission security, authentication mechanism, and sort of exception handling, for it could prevent the server from certain denial of service attacks
- ***Web Server*** and ***FTP Server*** shall support authentication and configuration interfaces for administration use.
- ***SSL*** supports secure data transmission.
- ***Application Firewall*** protects server from malicious connection that may terminate system services.

Web Server Security: Concerns & Approaches

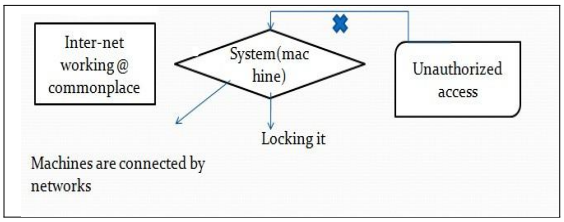
Web-Server security can be divided into three main areas of concern. One of these areas, **Network Security**, is primarily concerned with keeping unauthorized users from gaining access to the system. The second area, **file system security**, is concerned with preventing unauthorized access, either by legitimate users or crackers, to the data stored in the system. The third area,

Process monitoring deals with process activities and behavior of process flow in kernel level and looks for effectiveness and the efficiency of processes.

WSP: Network Security

As trends toward inter-networking continue, most sites will connect to one of numerous regional network, Most of these regional network are also interconnected, forming the Internet.

User of machine can access other hosts and comm. with other users around world Same way other hosts and users from around world can access your machine and attempt to break it, Mechanism is shown as in Fig.



File Security System: Monitoring

In computer systems information is stored traditionally in the form of files. File is considered as a basic entity for keeping the information. In unix-like systems, the concept of file is so important that almost all input/output devices are considered as a file[14]. Therefore the problem of securing data or information on computer systems can be defined as the problem of securing file data. It is a well accepted fact that securing file data is very important, in modern computing environment. Mechanism is shown in block diagram:

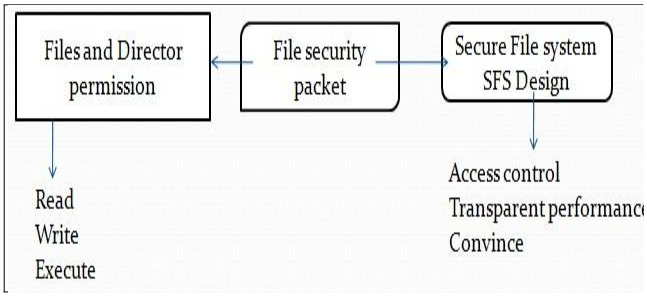


Figure:7

Drawback of Separate Mechanism of Monitoring /Profiling Techniques

- More volume of traffic
- It tap all the unnecessary events too
- It has no alert mechanism
- More memory required
- It has no feature of synchronization

Once After carrying out all the security concern and getting a efficient Web server protected profile in terms of a desired script, then It can be implemented as one of the many ways shown in Fig.

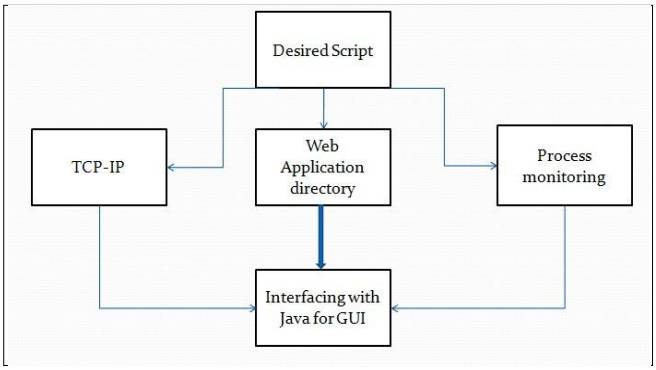


Figure: 8

V. CONCLUSION

A detailed and focussed study has been carried out in this paper with methodologies and approaches on web server security profiling including its all concerns, advantages as well as disadvantages. This detailed thesis and study will definitely be fruitful further for design and realization of such framework for secure web server for tracing various events of web server in order to detect any malicious attack on web server which helps in reducing threat of attacks on web server in real world.

Acknowledgement:

The author sincerely thank Sh. Tapas Kumar, HOD CSE, Dep. Lingayas University, Faridabad for his encouragement to carry out work. The author also would like to thank Utkarsh Tyagi, Abhishek Shukla for their support, motivation & valuable discussions.

References:

[1]. Dustin Lee, Jeff Rowe, Calvin Ko, Karl Levitt," **Detecting and Defending againstWeb-Server Fingerprinting.**

[2]. Aviel D. Rubin *(*AT&T Labs), Daniel E. Geer Jr. Certco,"A Servey of Web Security .

[3]. A.D. Rubin, D. Geer, and M.J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, New York, 1997.

[4]. Jared Karro, Jie Wang," Protecting Web Servers from Security Holes in Server-Side Includes.

[5]. Sheng-Kang Lin ," From Web Server Security to Web Components Security.

[6]. Christian Gilmore, David Kormann, and Aviel D. Rubin –Secure Remote Access to an Internal Web Server,‖ IEEE Network, Val. 13, Issue 6, pp. 31-37, Nov.lDec., 1999.

[7]. Dustin Lee, Jeff Rowe, Calvin KO, & Karl Levitt, detecting & defending against web server Fingerprinting, II In the 18-Annual Computer security Application Conference (ACSAC'OZj, pp. 321-330, Dec. 9. 2002).

[8]. 8) **S.** Jiang, **S.** Smith, and K. Minami, –Securing Web Servers against Insider Attack,‖ In the 17_h Annual Computer Security Applications Conference (ACSAC'OI j, pp. 265-276,

[9]. Jane Curry."Methods of monitoring processes with Zenoss Draft. www.skills-1st.co.uk

[10]. JJ.G. Steiner, C. NEuman & J.I. Schiller-Kerberos: An Authenticatin service for open Network Systems, II Proc. Winter 1988 general Conf. USENIX Assoc., Berkeley, Calif. 1988, pp. 191-202.

[11]. M.K. Reiter and A.D. Rubin, –Crowds: Anonymous nWeb Transactions,‖ *ACM Trans. Information Systems Security*, Apr. 1998; see also http://www.research.att. com/projects/crowds.