International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P) Volume-8, Issue-4, April 2018

Detection of Firewall Fingerprinting and Vulnerability Prevention by Denial of Attacks on Web Application

B.Prakash, P.Jyothi Lakshmi

***Abstract*— Firewall is a critical device that acts like a gatekeeper, watching the network and inspecting each packet to ensure it meets network security policy before it is allowed to pass. We think firewall is secure but it's not, many vulnerabilities compromise the firewall. Intruders exploit the firewall mainly host based using malicious scripts and access the server or web applications. In this paper, the concept of firewall fingerprint is assumed and the domain details like domain name, registrar URL, domain creation date, registrant address and server name of any web application is fetched. Also, the denial of most common attacks namely Cross Site Request Forgery, Remote File Inclusion, Cross-Site Scripting and Path traversal on web application is achieved. Even if the firewall is been compromised, intruder cannot access the files in the application or server as the application is made secure against most common vulnerabilities.**

***Index Terms*—Firewall, network inspection, URL, Fingerprint.**

I. INTRODUCTION

Today there are several computer system threats that come in many different forms. Some of the most common threats today are software attacks like Cross-Site Scripting, Path traversal, File Inclusion, Cross-Site Request Forgery,Data breach,Buffer overflow and memory corruption. Eventhough firewall protects against many vulnerabilities, the server details or the web application is not secure.

The unethical user can access the web application by different kinds of attacks. For example, in cross- site request forgery the packets between the client and the server can be modified easily. In path traversal attack, the root file from the server can be accessed easily as a result the server configuration file can be modified and in the file inclusion attack, if the server executes the injected file, the hacker can get the full control of the application. The proposed system overcomes the above mentioned issues in an efficient way. The system provides efficient domain fingerprinting as the details of packets in firewall is fingerprinted by fetching the details like domain name, registrar URL, creation date, registrant address and the server name. The port check is also performed by the system to know the network status.

Now, along with the fingerprinting, the system also provides denial of most vulnerable web attacks like Cross-Site Request Forgery, Remote File Inclusion, Cross-Site Scripting and Path traversal.

B.Prakash, Department of Computer science and Engineering, Adhiparasakthi Engineering College, Chennai, India

P.Jyothi Lakshmi, Department of Computer science and Engineering, Adhiparasakthi Engineering College, Chennai, India, Mobile No.9840628691

II. RELATED WORKS

A. Remote Operating System Fingerprinting Tools

Web applications are typically developed with hard time constraints and are often deployed with security vulnerabilities. Automatic web vulnerability scanners can help to locate these vulnerabilities and are popular tools among developers of web applications. Their purpose is to stress the application from the attacker's point of view by issuing a huge amount of interaction within it.

B. Path traversal patterns in a web application

Original sequence of log data is converted into a set of maximal forward references and filters out the effect of some backward references which are mainly made for ease of travelling. Algorithms are derived to determine the frequent traversal patterns. The algorithms are mainly of hashing and pruning techniques.

III. SYSTEM ARCHITECTURE

The overall features of the software are concerned with defining the requirements and establishing the high level of the system. The major software components are identified and decomposed into processing modules and conceptual data structures and the interconnections between the modules are identified.

A. Architecture model

This system fingerprints the domain details of the web application and displays the network status thereby uses the concept of firewall fingerprinting as how the firewall manages each packet with in the network traffic.

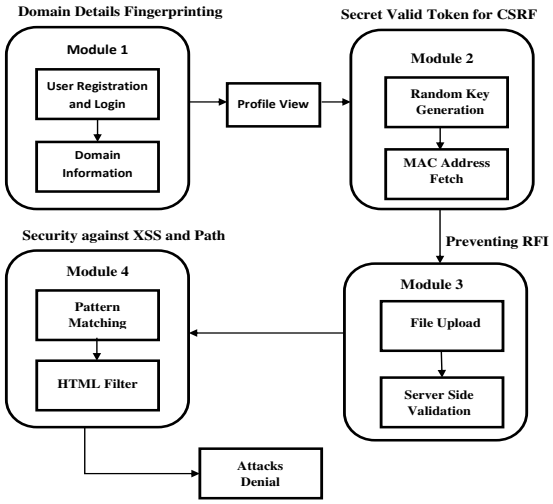

Figure1. Architecture diagram

IV. SYSTEM MODULES

A. Fingerprinting the Domain Details

The system allows the user to register by providing the user information. The user then logs in by providing registered username and password. When the unauthorized user access the application, the domain details along with the port details i.e. the network status can be fetched.

B. Secret Valid Token for CSRF

CSRF – Cross-Site Request Forgery is a type of attack that occurs when a malicious program causes a user's web browser to perform unwanted actions so that the application is hacked.

To avoid CSRF, a secret valid token is generated with below keys consideration,

Hash of User ID: A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.

Session Id: Session ID or session token is a piece of data that is used in network communications to identify a session, a series of related message exchanges.

Tokens with hash value: It is a unique identifier, usually in the form of a hash generated by a hash function that is generated and sent from a server to client to identify the current interaction session.

.

C. Preventing RFI

This system has a special feature to prevent RFI – Remote File Inclusion by three key ways,

1. Never use arbitrary input data in a literal file include request.
2. Use a filter to thoroughly scrub input parameters against possible file inclusions.
3. Build a dynamic white list.

D. Security against XSS and Path traversal

The system achieves security against cross -side scripting using HTML Tag filter and Pattern matching. In Html Tag Filtering, filter all malicious TAG like <script>, <img> etc. Recently all types of web sites are under medium level security i.e. websites are created by using html tags hence it is easily bypassed by the hacker using those tags. In this technique all types special characters and previous attacking tags are filtered.

The security against Path traversal is achieved by preventing the access to restricted directories and for the execution of commands outside the web server's root directory.

V. METHODOLOGY

A. MD5 Technique

The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input. MD5 is used in many situations where a potentially long message needs to be processed and/or compared quickly. The most common application is the creation and verification of digital signatures. It is used as a checksum to verify data integrity.

The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words) the message is padded so that its length is divisible by 512. The padding works as follows, first a single bit, 1 is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264. This project uses MD5 to provide data integrity in password security.

B. SHA1 Technique

The SHA-1 algorithm belongs to a set of cryptographic hash functions similar to the MD family of hash functions. But the main difference between the SHA-1 and the MD family is the more frequent use of input bits during the course of the hash function in the SHA-1 algorithm than in MD4 or MD5. This fact results in SHA-1 being more secured compared to MD4 or MD5 but at the expense of slower execution.

The SHA-1 algorithm produces a condensed representation of the given input message or data file. This input message is considered as a bit string where the length of the message is the number of bits in the input string. The purpose of message padding is to produce a padded message of length equal to a multiple of 512 bits. The reason behind this is that the SHA-1 algorithm processes messages as 'n' number of 512-bit blocks when computing the message digest

The original message is initially appended with a '1' followed by a number of '0' bits such that the resultant length is 64 bits short of the next highest multiple of 512 bits. The last 64 bits of the last 512-bit block are reserved for representing the length of the original unpadded message. The result of message padding is a padded message containing 16*n words for some n>0. Here in this project SHA-1 is used in random key generation.

.

VI. CONCLUSION

In this paper, the implementation is done for the system that fingerprints the domain details and fetches the network status. The system mainly detects and denies the most common vulnerable attacks. The user has to register and then login using valid registered username and password to detect and deny the attacks.

REFERENCES

[1] B. Mewara, S. Bairwa, J. Gajrani, "Browser's defenses against reflected cross-site scripting attacks", International Conference on Signal Propagation and Computer Technology (ICSPCT), pp. 662-667, July 12-13 2014.

[2] Muhammad Shahzad and Alex X. Liu, "Noise can help: Accurate and efficient per-flow latency measurement without packet probing and time stamping", in Proceedings of the ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), Austin, Texas, Hune 2014, pp. 207–219.

[3] Cisco˜PIX Firewalls, "http://www.cisco.com/", 2011.

[4] Swati Ramesh. Kesharwani, Aarti. Deshpande, "A Survey On XML-Injection Attack Detection Systems" in International Journal of Science and Research (IJSR), 2012, ISSN 2319-7064.

[5]Cenzic Web Application Security Trends Report—Q3—Q4 2009, 2010.

AUTHOR'S PROFILE

B.Prakash received the B.E. Degree in Computer science and Engineering from Adhiparasakthi Engineering College, Anna University, Chennai, India in 2006. Received M.E. Degree in Computer Science and Engineering at Sri Krishna Engineering College, Anna University, Chennai, India in 2009. His research interest includes wireless sensor network.

P.Jyothi Lakshmi received the B.E. Degree in Computer science and Engineering from P.B. College of Engineering, Anna University, Chennai, India, in 2010. Currently doing M.E. In Computer Science and Engineering at Adhiparasakthi Engineering College, Anna University, Chennai, India.