International Journal of Allied Practice, Research and Review
Website: www.ijaprr.com (ISSN 2350-1294)

PORT KNOCKING: A Solution to the Firewall Network Security

Poonam Verma and Poonam Malik
Jagannath Institute of Management Sciences
Lajpat Nagar, New Delhi

Abstract - In the present day scenario, there has been an information explosion, which has been the by product of the internet popularity. However, the internet has also opened new avenues for the hackers to control various sensitive information and details of individuals or organizations to their profit end.

Various techniques have been used to spoof IP addresses, hijack the web browsers or gains complete access to a networks. Firewall has been one of the most popular techniques used by the individuals or organizations for security purposes. However the rapid growth in the field of technology results into new methods adopted to break the security trapdoor of the firewalls. In order to protect the organizations or individuals who do not use public HTTP and SMTP, a technique of Port Knocking is adopted.

In the present paper, we would like to explore the various features of the firewall. We would further extend the paper to the new approaches such as Port knocking and its implementation methods.

Keywords: Firewall, Port Knocking

I. Introduction

A firewall is a collection of security measures designed to stop unauthorized electronic access to networked computing system.
It is used to shield private networks & people machines from the risk of the great internet, a firewall can be utilized to filter incoming and outgoing traffic based on a predefined set of rules known as firewall policies.

Packet flowing through a firewall can have one in all the three outcomes:-

1. Accepted—allowed through the firewall

2. Dropped – not allowed through with no indication of firewall.

3. Rejected – not allowed, in the course of an attempt to inform the source, then the packet was rejected.

Types of firewalls

1. Packet filters (stateless):- if a packet matches the packet filters set of rules, the packet filter can drop or settle for it.

2. State full filters: it enlists records of all connections passing through it and might confirm if a packet is either the beginning of latest connections, a part of already available connection or is a packet with no validity. It can tell when packets are part of legitimate session originating among a trustworthy network. Stateful firewall maintains tables contain data on every active association node, including the IP address, ports and sequencing numbers of packets.

3. Application layer:-

   i) It works sort of a proxy. It will "understand "certain applications and protocols.

   ii) It might examine the contents of the traffic obstruction what it views as inappropriate content.

Policies utilized by firewall to handle packets are based on many properties such as:-

1. TCP or UDP
2. IP address at the Source Node and destination Node
3. Source and destination ports
4. Application payload of the packet.

There are two basic approaches to form firewall policies (or rule sets) to effectively minimize vulnerability to the surface word whereas maintaining the required function for the machines within the trustworthy interval network.

(a) White list approach: - a safer approach to outline a firewall resulted is that the default-deny policy, within which packets are dropped or rejected unless they are particularly allowed by the firewall.

(b) Blacklist approach:-All packets are allowed through except those that for the rules outlined specifically in the protocols defined for the blacklist. This kind of configuration is additionally versatile in making sure that service to the internal network is not non continuous by the firewall.

The firewall has two configurations:-

Two routers that do packet filtering & also support from an application gateway.

- Every packet should transit two filters and an application gateway to travel the data packets in or out.
- Each packet filter may be a customary router equipped with some further practicality.
- The additional functionality permits each incoming or outgoing packets to be inspected.

- Packet meeting some, criterion are forwarded unremarkably. The data packets that fail the test are marked for the removal from the channel.
- The packet filter on the inside surface computer network checks outgoing packets and the one on the surface Computer network checks incoming packets.
- Packets crossing the first hurdle head to the applications gateway for additional examination.
- Packet filters are usually driven by the tables configured by the system administrators.
- These tables list sources and destinations those are acceptable.
- The table also lists particularly those machines or IP addresses that are not permitted to be send request or receive data from. IT also enlists criteria for these blocked machines.
- Using these tables stateful firewalls will enable solely incoming TCP packets that are in response to a connection initiated from within the interior network.

Problems in Firewall security modes:

With the inflated use of the web, the scams relevant, to the web has also inflated. For Eg: IP spoofing, that is additionally referred to as forgery of IP address and it is a hijacking technique in which the hijacker masks as an authenticated user and conceals their identity, spoof a internet site, hijack the net browsers or gains complete access to a networks. The overall technique behind is that IP address of a legitimate host is received and it alters the packet headers in order that the legitimate host seems to be the source and receives all the packets which can be forged. It is also known as host file hijack or attack on the center man.

When IP spoofing is employed, to hijack a browser by taking complete management of the legitimate webpage - This in consequent action will lead the users to the fallacious Web Page that helps the hacker to collect the useful details of the users and then later use it for further more difficult fraud tasks. Eg: if an Indian post government site is spoofed, then the users logging into the URL of the Indian post will be lead to the spoofed website that contains all the content created by hacker. All the main points that are fed in by the users can be used by the hackers to further obtain the account details in post office. Further these details can be used to be part of the zombie army that sends the mails in bulks to the authenticated users to gain access to their accounts (Spams in email).

Users and administrators can shield the access to their approved accounts by putting in and implementing firewalls that block outgoing packets with the source addresses that disagree from the IP address of the users' computer or internal network.

One of the approach adopted on firewall in computer networking is Port Knocking and it is a technique of outwardly opening ports by generating a association try on a group of pre-nominated closed ports. Once the sequence of knocks for a particular port is matched with the saved knocked pattern the firewall gateway permits the connections to be made to the requested port and to retrieve the required data.

The problem today in the world jam packed of security threats, it ought to be assumed that all traffic is monitored by an unknown third party as it travels across a network. However, we should be also be additionally aware that our knock sequence are often positively ascertained by an eavesdropping person in the middle of our connection and simply reply the knock sequence to get the same response from the server (open port or perform a task). This downside is called "TCP Replay Attack". So a replacement resolution has to be found, where the knock sequence is not re-playable.

Port Knocking

Port Knocking is an authenticated method used to grant remote access without leaving a port open for a long span, due to which it becomes easier to handle the port scanning and it helps to control access to computers or other network devices. It permits the user to know a "Secret knock" that is required to identify the authentication pass which helps to perform a sequence of connection attempts. For every IP address, there is a specific pattern of knock. There exists a small program named daemon that helps to monitor the connection requests and determines whether a client can perform the correct knock pattern or not, if the user is able to clear the knock pattern then the user is permitted to find the required files. The daemon runs on the server that is in parallel runs manipulations to monitor the connection attempts.

The daemon that deals with the knock is located at the low level of the TCP/IP stack and is potentially invisible to the intruders. However the port knocking has its own set of challenges like man-in- the –middle attacks and thus cannot be completely relied upon for the authentication purposes.

The present problems with the previous developed techniques for port knocking is that the captured tokens can be replayed due to which the security can be easily breached. Some of the problems with the existing firewall port knocking are as below:

A) Network Address Translators :

If traffic passes through NAT and if the public IP address is encoded in the token, then the port will be opened to all the hosts sharing the same public address

B) Lack of Logical Association :

When the lack of the logical association between the authentication sequence and the connections that are opened once the port is clear after the security check, where the hackers can block the future transmissions of other authenticated clients

There are three ways that messages that could be send from an authenticated user through a server and the communication through

- An Open port
- A Closed port
- Covert channel

If the authentication mechanism requires the server to respond then this may be send from a port that is closed immediately after sending and does not receive any incoming messages.

Port sequence which requires a shared secret between the user and the server , and it should not be made public. If a client transmits packets to a specific sequence of servers, then the server will perform some action such as opening and only with the help of Port Sequence.
Three applications of the port sequence are:

a) transmit a plain text authentication token
b) application that transmit a cryptographic knowledge
c) transmit a OTP.

II. IMPLEMENTATION

Port Knocking is a filter which, filter outs the unauthenticated users from the authenticated ones along with maintaining IP rules. However this approach cannot be used with the public services as it will be vastly known how to generate the knock sequence, leaving little for the protection from the intruders.

Step 1: Assume that users are unable to connect to any ports in the network.

Step 2: Those authenticated clients who had prior knowledge about the port knock pattern will try to get synchronized to the applications running in the server; however no acknowledgement is received during this time.

Step 3: Port knocking daemon analyses the attempts made by the clients to make connections and decrypts the knocking pattern.

Step 4: Only those clients that are able to pass this test, are permitted to enter through the firewall to connect to the required port and access the data.

III. Limitations

Port Knocking interfaces with the server's IP stack. It is necessary for the knocks to come back as a series of the associated nodes attempts to connect.

IV. Proposed alternatives to port knocking

As we are aware that there is no logical sequence that is followed in case of the port knocking, therefore if the port knocking is combined or replaced with the set of security questions adopted for authentication for transaction in banks , this would remove the limitations posed by the Port Knocking . It will require an application to be designed that permits the users to write their own questions and save that dataset into the database/ back end of the application, which will be useful to match the answers at the authentication time.

V. Conclusion

We in this article have tried to explore a method of asking a combination of questions while port knocking , thereby providing a method of authentication with some logical sequence which is missing in the port knocking sequence.

VI. References

1. Amir R. Khakpour, and Hakima Chaouchi, *ESSTCP: Enhanced Spread-Spectrum TCP in Proc.* of the 3rd International Workshop on Security in Systems and Networks (SSN'07) in conjunction with IPDPS 2007, Long Beach, CA, March, 2007.
2. Churchouse.R.F , 2001.Codes and Ciphers: Julius Caesar, the Enigma, and the Internet .
3. Doyle M Implementing a Port Knocking System in C, 2004. *Department of Physics, University of Arkansas*
4. Menezes.J, A. 2001. *Handbook of Applied Cryptography*. 586
5. Mao, W. 2003**.** Modern Cryptography: Theory and Practice
6. Narayanan ,A. 2004. *NewsForge.* A critique of port knocking,

7. port knocking. *Wikipedia*

8. Port Knocking - A new trend for firewall administrators. *TLANews.com*

9. Schneier. B, 1996. *Applied Cryptography*. John Wiley & Sons