Knowledge Based Handling Linux Firewall: Help System

Jayakumar. S[1] Mohan Kumar. R[1]
[1]*Master Of Computer Application,*
[1]*Sacred Heart College, Tirupattur, Vellore [Dt],Tamilnadu,india.*

Abstract

Linux firewalls it's a wide availability and open architecture which provides a suitable and convenient for expert command line user interface. We hope that the existing firewalls are in a formal usage, yet practical, there is need of knowledge based scheme for LINUX firewalls towards building a higher-level active help system. The problem of how to accurately recognize the users commands and applications, to block up the unrecognized users query with potential safety hazards. In case the current firewalls cannot effectively adapt to the huge change of network configuration, the knowledge base can assist to the users. Based on the knowledge base the next generation of firewalls and its configuration takes the instant information and give knowledgeable advice to the expert command users.

Keywords- Users Command, Application, Linux Firewall Configuration

1. Introduction

Basically Firewall designed to protect network traffic; connections and prevent unauthorized access of private and public network service [1]. However, Linux firewall provide full-fledged secure network access, with in that nowadays we facing rapid development of computer network and internet accessibility, technology issues, too much of updates on softwares and hardware component. On the other hand we were handling various of unsecure access attempt to unauthorised information, such as viruses, junk mails, etc.

In future too much of updates and junk file can be overlap the actual firewall, or if any new network technology adapted to firewall architecture means firewall may not be understand or it does not provide more effective internet, file sharing access, it can not perfectly identify the user commands application interactions and firewall configuration. Our approach to give knowledge based handling Linux firewall to give help system for expert command user.

2. Command Line User

Linux/Unix operating system use various command that the user can enter query and accomplish their operation. Shell commands various from one shell command to another [2]. Power users, who are always looking for ways to maximum the amount of work accomplished with a minimum amount of time.

Example

There are number of GUI tools for configure iptables, both free and commercial. For redhat, the iptables configuration file is /etc/sysconfig/iptables which is used by /etc/init.d/iptables startup script Iptables – administration tool for IPV4 packet filtering and NAT.

Iptable [-t table] –[ADC]chain rule-specification [option].

Here propose a Knowledge based Firewall Administration Tools which is most uesfull for Linux firewalls.

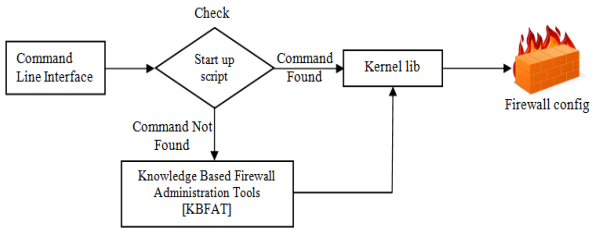

Fig 1: KBFAT process

3. Data leakage

Determining where and how data may be leaking from a network is a difficult problem. It is problem of intrusion detection-how do you sort a very small event from a vast mass of larger ones? Our answer was to look that might indicate a deeper problem, using a tool we develop called

"KBFAS"-Knowledge Based Firewall Administration Tool [3].

3.1 Knowledge Based Firewall Administration Tools [KBFAT]

A knowledge base is special kind of database for knowledge management. A knowledge base is information to be collected, organized, shared, searched, and utilized. It can be machine readable or intended for human use [4].we have classified KBFAT as three components.

- Knowledge collector
- Knowledge analysis
- Knowledge representation
- Knowledge finalizer [KDS]

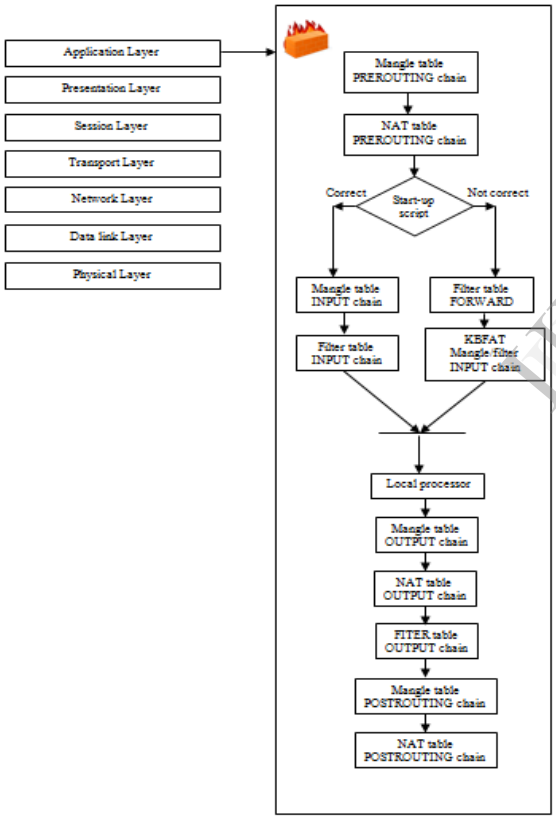

Fig 2: mangle process table for KBFAT

Algorithm 1:

BEGIN
ENTER "COMMAND" //enter command in terminal window
PASS "COMMAND" INTO "STARTUP_SCRIPT"
IF "command && arguments "
//check "command && arguments"
THEN
DO KERNEL_LIB;
ELSE
MOVE COMMAND INTO KBFAT; // it check the possibility of command, the user expect result in knowledge base expert user command.
RETURN "KERNEL_LIB"
PROCESS COMMAND //process the command and get desired output of knowledge based one.
END

3.1.1 Knowledge collector

It is responsible for to gather data from shell command line. Whenever the user entered the query which is watching through History command. Iptables/Netfilter is the built-in filter in most Linux releases. Iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of number of classifiers. This combination of works well when applied in personal computer or small-scale LAN. But when it comes to Large network, the performance of the Iptables/Netfilter is quite poor[5].

Because hardware may be not supported and firewall configuration could not adapted to new technology by itself. If It is possible to occur some operation could not complete the knowledge analyser can take this query to knowledge base

3.1.2 Knowledge analysis

Knowledge Analysis is an approach to analysing problems, issues or events through a knowledge perspective in order to understand them at a deeper level and form new insights about them[6].

Expert command user always preferred with complex operation are done through different commands that is way of thing might be effective action and also some time it will arise deadlock problem. The knowledge analyser analysis the user entered query as a objet and it is preferred with kernel library Within that we move to knowledge based analysis is an approach to analysis given command should be in correct form and also check with arguments.

3.1.3 Knowledge representation

Knowledge representation involves analysis of how to accurately and effectively and how best to use a set of commands, arguments to represent a set of facts within a knowledge base.

```
RULE: 1
----------
BEGIN              //query take copy from kernel
library
IF "COMMAND && ARGUMENTS" ==
"REAL_OBJECT"
THEN
        PRINT "some what found DO YOU
WANT PROCEED WITH YOUR QUERY (Y/N)"

        IF "QUERY" != "NOT POSSIBLE
        QUERY OPERATION"
        THEN
                PRINT "OPERATION
SUCCEED"
        ELSE
                PRINT "OPERATION NOT
SUCCEED"
END
```

Here, Real_object – refer with kernel library file Because we should check the query whether real or not.

3.1.4 knowledge detection system [KDS]

Traditionally, firewall having intrusion detection system (IDS) architectures was examined and also discarded data rather than auditing data . In KDS the data can be analysed as knowledge object by the help of knowledge base and KDS architecture support to the expert user[7]. Here our approach of knowledge based on detecting techniques affect the knowledge build up firewall more effective manner with knowledge based firewall admission tools that the specific problem of contain 1. User enter commands 2. Application 3. Firewall configuration. This detection system contains knowledge about firewall When such type of problem may raise, that time KBFAT respond and help to resolve problem on knowledge based.

Conclusion

On basis of analysis of the traditional firewalls, a new knowledge base content filtering firewalls based on the Iptables/Netfilter frame in Linux is realized this paper. We give knowledge based advice to shell command which improve the efficiency of command operation, reduce the delay and how to increase the network throughput. This KBFAT firewalls tool plays a good role in all open source Iptables/Netfilter, and greatly improves the work efficiency of the LINUX.

Reference

[1].http://www.kb.iu.edu/data/aoru.html

[2] Jayakumar, Mohankumar - "Knowledge Based Handling Linux Utility: Help System" IJERT ISSN: 2278-0181 Vol 2 issue 5, May – 2013 pages : 1385- 1388.

[3] Ronald, 'Executive Director, Warner Bros.Entertainment Inc'. Marcus Ranum, 'Chief of security, Tanable network security, Inc.' – "Someone To watch Over Me" - http://www.ranum.com/security/computer_security/

[4].http://www.linux.about.com/cs/linux101/a/cmd_shellcmd.htm

[5]. Xiao Long Dou, Jia Chun Li, Ling Zhang - The Research and Implementation of Transplanting the Iptables/Netfilter to an IXP2400 Based Firewall System.

[6]. Theknowledgeanalyst.com/blog/what-is-knowledge-analysis/.

[7]. LuXuanmin, Shan Chang Moses "Research on IP Addresss Replacement Technology Based on iptables".