Proposed Router Intrusion Detection and Protection Systems

Nareshkumar D. Harale* and Dr. B. B. Meshram**
*Department of Computer Science & Engineering, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India.
nareshkumar.d.harale@gmail.com
**Department of Computer Engineering and Information Technology, VJTI, Matunga, Mumbai (Maharashtra), India.
bbmeshram@vjti.ac.in

Abstract: Modern Attackers most of the time attack the gateway router's software and make the router to behave in a malicious way. This Paper focuses on various attacks and how these attacks will be detected successfully by router log analysis. This paper also illustrates the proposed software architecture, its data structure and algorithms for the detection and protection of the router intrusions. So in this way in proposed system, logs are used to detect attack and also give defense mechanism for the detected attacks. The main aim of the work is to give details about how to communicate with the router from the program to turn ON only needed debugging; Collect router logs in a separate Syslog server; Segregate log files based on protocols; Analyze the device log files to detect malicious attacks or misconfiguration; Communicate with the router again to apply appropriate access lists as defense mechanism and Save the logs report. Due to space constraints, some of the screen shots are shown. This work looks at some of the techniques to improve the accuracy of automated log analysis and make it a cost-effective tool for network management and improving network reliability.

Keywords: System Integrity, Router Configuration, Network Security, Routing Systems, Routing Algorithms, Router Intrusion Detection Systems, Router Intrusion Protection Systems.

Introduction

Cisco routers can provide an immense quantity of real time status information to support network management simply by enabling the system logging facility. Every state transition of every line can be recorded, along with call statistics, router configuration changes, software errors, environmental warnings, IOS reloads, and more. This level of detail can provide valuable insight into network operation that goes far beyond its normal use as a tool for resolving the cause of network failures. Many classes of problems, such as weak links which fail intermittently for brief periods, will show up in the syslog long before they are noticeable to users. Given the valuable information and operational insight available from the system logs, detailed analysis of syslog data should be a routine part of every network administrator's job. Even if there are no failures to report, routine testing of dial backup links will generate log entries which still must be scanned to ensure that they all really are test results and not a problem which just happened to occur during test periods.

Sawmill [16] is a Cisco Systems Router log analyzer (it also supports the 905 other log formats listed to the left). It can process log files in Cisco Systems Router format, and generate dynamic statistics from them, analyzing and reporting events. Sawmill can parse Cisco Systems Router logs, import them into a MySQL, Microsoft SQL Server, or Oracle database (or its own built-in database), aggregate them, and generate dynamically filtered reports, all through a web interface. Sawmill can perform Cisco Systems Router log analysis on any platform, including Window, Linux, FreeBSD, OpenBSD, Mac OS, Solaris, other UNIX, and others. Log analysis (or system and network log analysis) is an art and science seeking to make sense out of computer-generated records (also called log or audit trail records). The process of creating such records is called data logging. Typical reasons why people perform log analysis which includes Compliance with security policies , Compliance with audit or regulation ,System troubleshooting, Forensics (during investigations or in response to subpoena), and security incident response. Logs are emitted by network devices, operating systems, applications and all manner of intelligent or programmable devices. A stream of messages in time-sequence often comprises a log. Logs may be directed to files and stored on disk, or directed as a network stream to a log collector. Log messages must usually be interpreted with respect to the internal state of its source (e.g., application) and announce security-relevant or operations-relevant events (e.g., a user login, or a systems error). Logs are often created by software developers to aid in the debugging of the operation of an application.

Literature Survey

There are few methods as well as robust algorithms which used for detection of router level attacks are given below:

Port Scan Attack - An attacker can run a port scan on the router to see which ports are ON and which are not. This is mostly the first step for an attack. The display variable is used to prevent the announcement of attack more than once for the same attack. The flag variable is used to start a fresh new scan for the attack Unknown Login Attack -Some attacker can somehow get router's access via telnet over the network and try to do malicious activity inside the outer. Telnet attempts on the router can be detected by log analysis.
ICMP Redirect Attack -ICMP redirect packets are actually sent by routers to hosts if they find a better path to reach a destination. If a router receives a packet and forwards the packet to the same interface where it had received then an ICMP redirect can be sent. But an attacker can carry a man in middle attack using redirects. Use the following regular expression to detect ICMP redirect attack.
BGP Session Termination Attack -TCP reset attack is the attack in which a TCP connection is terminated by the attacker using a spoofed packet with the RST (reset) bit in the TCP packet set. This attack affects BGP protocol. Use the following regular expression to detect BGP session termination attack.
OSPF Hello Packet Deletion Attack- OSPF neighbors exchange hello packets every 10 seconds (Default hello timer is 10 seconds.) When 4 consecutive hello packets are missed by an OSPF process, then the OSPF process declares its neighbor as dead (Default dead timer is 40 seconds.) When a neighbor is dead, its entries will be flushed from the routing table. Attacker can purposely delete OSPF hello packets. After 4 consecutive message deletions, the neighbor ship will break. This is an attack which has caused the OSPF neighbor ship to break resulting into flushing of its OSPF entries.
OSPF DR BDR Null Attack- OSPF is a victim of DR, BDR null attack. OSPF elects DR, BDR on a multi access network. DR, BDR are elected based upon the priority and router ID (highest loopback address) sent in the hello message. After the election is done, the elected DR, BDR are sent in the hello message. An attacker can create a phantom router with highest priority and ID. Attacker will now set DR, BDR to null and then send that hello message. This will force reelection for DR, BDR and will elect the phantom router ad DR which will create undesirable effect. Use the following regular expression to detect DR BDR null attack.
Router Intrusion Protections by Configuring ACLs' - Snort is an open source tool which works as an IDS (Intrusion Detection System).In this attack on router is prevented by the use of Snort to generate alerts for attacks and configure ACLs to defend. Snort can also be used to detect any intrusion in router and also took measures to take action for that intrusion using ACLs Rules are written in Snort and they are matched against the packets. If a packet matches then messages are sent to the snort log. These logs now can be studied and appropriate access control lists can be generated for the router to curb the attack.

Proposed System's Software Architecture

The software architecture design of the proposed system further dictate the design of essential Data Structure as well as Algorithms used for its successful implementation.

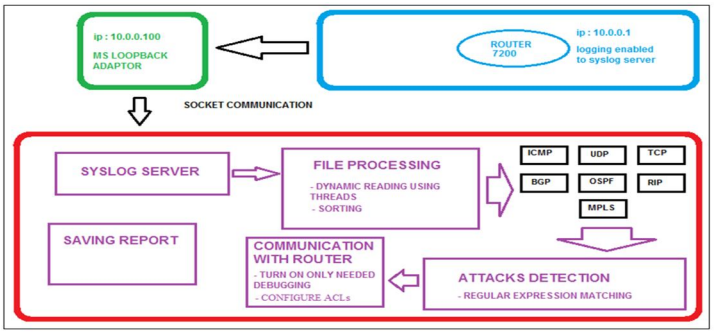


Figure 1: Software Architecture for Router Log Analysis System

the file processing module starts thread to read and sort and detect attacks from a continually updating file; the communication with router module has the burden of holding socket communication with routers when commands need to be fired; the Syslog server program is continually receiving UDP packets at port 514. Security monitoring software's do require a high configuration system all above component can be simulated in one system for testing.
The blue box represents a GNS3 instance. A router is running in that instance
The green box represents an MS LOOPBACK ADAPTER i.e. used to connect the java project with the router
The red box represents the entire java software. It contains the following modules such as Syslog server module, File processing module, Attacks detection, Communication with router, and saving report modules.

Software Architecture Components and their Interaction

This section is describing the detailed software architecture design requirements of the proposed systems. The depicted component diagram is used to model physical aspects of a proposed system. Physical aspects are the elements like executables, libraries, files, documents etc. which resides in a node at the time of program execution.

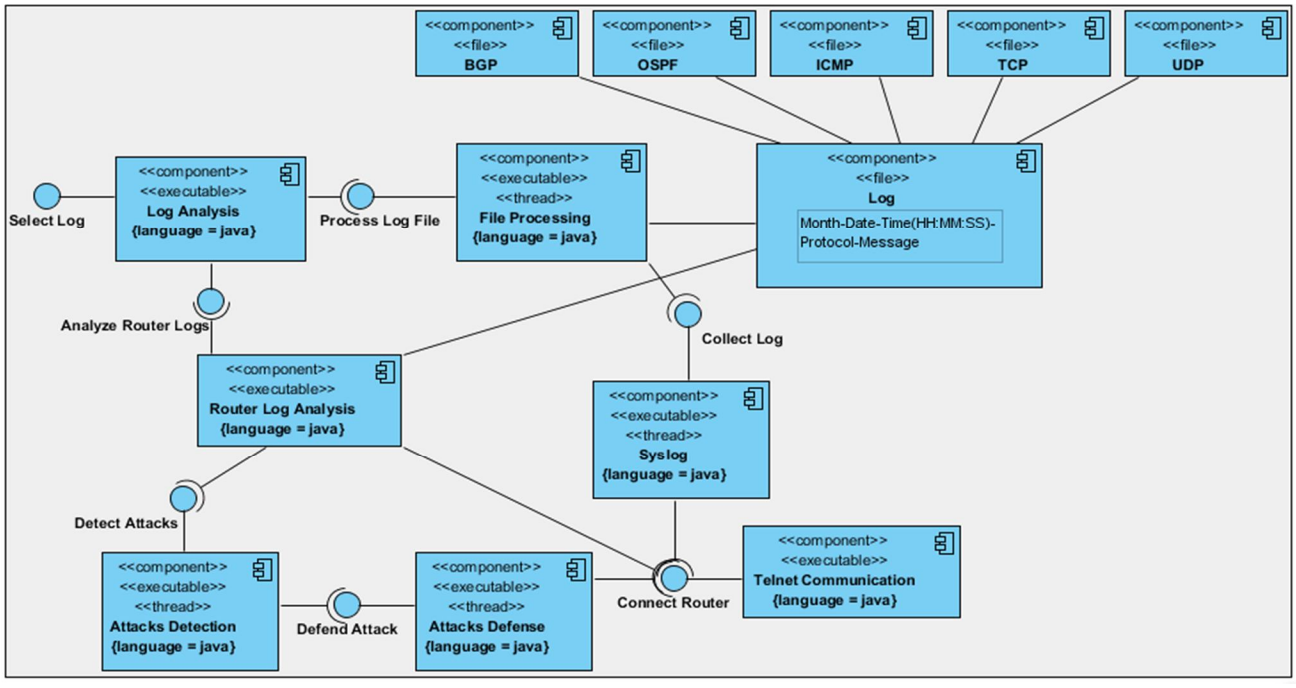


Figure 2: Software Architecture diagram for Router IDPS Systems

Data Structure and Algorithms Design

In this section, we have described the various data structures as well as algorithms used for proposed router intrusion detection and protection system implementation.

Data Structure Design

Below given table is representing the data structures used by proposed system in order to implement the log analysis and file processing, attack detection and protection of the attacks.

Table 1: Data Structures used by Router IDPS

Module name	Stereotype	Algorithm	Data structure Design
Log Analysis	<<executable>>	-	-
File Processing	<<executable>>	File Processing Algorithm	-
Log	<<file>>	-	File Fields :-Month-Date-Time (HH:MM:SS)-Protocol-Message
Router Log Analysis	<<executable>>	-	-
Syslog	<<executable>>	Syslog Algorithm	-
Attacks Detection	<<executable>>	Port Scan Detection Algorithm Hello Deletion Detection Algorithm Regular Expression Matching Algorithm	-
Attacks Defense	<<executable>>	Communicate Router Algorithm	-
Telnet Communication	<<executable>>	Communicate Router Algorithm	-

Algorithms Design

Below section is emphasized on the design of the various algorithms used for proposed Router Intrusion Detection and Protection Systems.

Router Syslog Algorithm -The algorithm for syslog workflow implementation is as given below:

Algorithm : Router Syslog Algorithm
Input: fos //FileOutputStream
Output: realdata //byte array containing logs
Algorithm**:**

1. Create DatagramSocket for UDP port 514
2. Create DatagramPacket with buffer size of 10000 bytes
3. Create a file to store all the logs using FileOutputStream
4. While (True)
   a) Receive packet using the create socket
   b) Get the data from the packet into byte array
   c) Write the byte array into the file , Exit

SysLog File Processing Algorithm - Java's regular expression matching is very strong [11]. It contains an entire package called java.util.regex dedicated to regular expression matching. The main classes used are Pattern and Matcher.

Input: input //RandomAccessFile pointing to syslog file
Output: bgp //FileWriter pointing to bgp logs
tcp //FileWriter pointing to tcp logs
udp //FileWriter pointing to udp logs
icmp //FileWriter pointing to icmp logs
ospf //FileWriter pointing to ospf logs
rip //FileWriter pointing to rip logs
Algorithm:

1. Start a Java thread and do the following inside the thread
2. Open the syslog file for processing
3. Create varisos patterns for regular expression matching
4. Read the syslog file line by line , For every line in the syslog file do the following :
   a. Match the line against all the patterns
   b. Open the pattern is matched
   c. Open the appropriate file in append mode
   d. Write the log entry in that specific file

Once some pattern is matched , don't try for the remaining patterns, Directly go to next line Step 3

Port Scan Detection Algorithm - The algorithm for detecting port scan attack is as given below:

Input: line //syslog line
Output: alert //port scan attack alert
Algorithm:

1. Write the pattern for matching the TCP listen log entry. The source and destination IP will be hardcoded here. The destination port will be a variable.
2. If the pattern is matched
   a. Extract the time into time variable
   b. IF flag ==0 then
      i. Initialize *counter* =0
      ii. Copy time into *timestamp*
      iii. Set *flag* =1

Else
i. Increment the *counter*
c. IF the *counter* > *threshold* and *display* = 0
i. Announce port scan attack and Set display =1
d. If current time is timestamp+120 second then
i. Set flag=0 and Set Display =0
3. Exit

OSPF Hello Packet Deletion Detection Algorithm

Input: line //syslog line
Output: alert //OSPF hello packet deletion attack alert
Algorithm**:**
1. Write the pattern for matching the OSPF Hello log entry.
2. Extract the *seconds* field of the time into *seconds_time*
3. When the first pattern is matched then
- Copy seconds_time into init_hello_time
i. Create an array times of size 6 of all possible seconds_time
ii. Match every hello log entry seconds_time with times[i].
4. If the values are not equal then Calculate number of hello missed using modular arithmetic method within the times array and Exit

Communication Router Algorithm

Input: Host //router's IP
Pass //router's password
Output**:** Socket //connection to the router
Algorithm**:**
1. Create a socket connection giving router's IP Address and port-23 for telnet
2. Get the reader and writer streams for this socket connection
3. Read lines from the socket continuously into *readchar*
4. Keep a record of last 5 readchar into readchar1, readchar2, readchar3, readchar4, readchar5
5. Check the end character of the readchar is Password, R1>,R1#,R1(config)#, R1(config-if)#, R1(config-std-nacl)#
6. Based on above end character and last 5 char , write appropriate command one line at a time using writer stream and Exit

Proposed System Implementation and Results

Proposed System Components

Syslog Server - Routers have very less memory. But logs generated by the router are huge and will require large space to store. If the memory becomes full then logs will be overwritten. We don't want this to happen because some logs are very crucial. So now the logs are successfully stored on the Syslog server to provide a clean separation. The router console will not be interrupted with logs now. The logs can be viewed on the separate machine having Syslog server. Log analysis can now be done on this machine.

Levels of syslog server logging: There are eight levels of logging. When a particular level is set, then all logs upto and including that level are generated. The command to set log level is 'logging trap level'. The eight levels are as follows:

Emergency (severity 0)—the system is unusable, Alert (severity 1)—Immediate action is needed, Critical (severity 2)—Critical condition, Error (severity 3)—Error condition, Warning (severity 4)—Warning condition, Notification (severity 5)—Normal but significant condition, Informational (severity 6)—Informational message, Debugging (severity 7)—Debugging message [7].

Deployment of Syslog server - The machine on which the Syslog server is running is connected to the core switch. In this way, all the routers can direct their logs to the Syslog server. This gives the network administrator control over monitoring all the routers. Along with Syslog server, few other modules will be deployed on the system. These modules are shown in Fig. in purple. The black box is the system having IP address 10.0.0.100. The router interface and this system should be in the same network in order to communicate.

File Processing - Above Syslog server program will write all the log messages received on UDP port 514 into a single file on the system. This process will be happening continuously. A Java thread will be launched which will do the task of the Syslog server [11]. So the Syslog file is continuously updating. This continuously updating file will be read by a file processing module. The file processing module is launched in a separate java thread. This module is continuously running. It will parse every line from the Syslog file and sort them into different files protocol wise.

Router Attacks Detection and Protection Mechanism

This section will focus on various attacks and how these attacks will be detected successfully by the system. This is the main aim for router log analysis: Attacks detection. Some attacks can be detected by just analyzing one log entry such as BGP's session termination attack or ICMP redirect attack. On the other hand, some attacks require analyzing more than 1 line before actually declaring that an attack has happened. Some of the algorithms used for detection of router attacks are given below:

Port scan attack

An attacker can run a port scan on the router to see which ports are ON and which are not. This is mostly the first step for an attack. Loopholes can found after a port scan.

Detection mechanisms of port scan attack	**Protection mechanism of port scans attack:**
The source and destination IP address will be same everywhere. The destination ports will be different. A threshold can be maintained by our algorithm which will tell how many packets to scan before announcing a port scan attack. This threshold might be 10, 15 as stated by the network administrator. The display variable is used to prevent the announcement of attack more than once for the same attack. The flag variable is used to start a fresh new scan for the attack. Distributed Denial of Service (DDoS) attack on the router can also be detected in the similar fashion. The regular expression pattern is as shown below:	Configure the following IP ACL Router>en Router#conf t Router(config)#ip access-list standard port_scan Router(config-std-nacl)#deny attackers_ip 0.0.0.0 Router(config-std-nacl)#exit Router(config)#interface f1/0 Router(config-if)#ip access-group port_scan in
(\\w+ \\d+ \\d+:)(\\d+)(:\\d+)(.\\d+:\\s+)(tcp0: I LISTEN)(\\d+.\\d+.\\d+.\\d+)(:)(\\d+)(10.0.0.1:)(\\d+) Attackers IP which can be extracted as matcher_variable.group(6)	

Unknown login attack

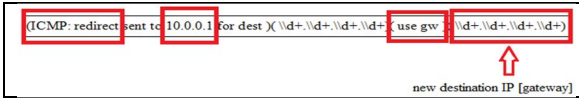
Some attacker can somehow get router's access via telnet over the network and try to do malicious activity inside the outer. Telnet attempts on the router can be detected by log analysis.

Detection mechanism of unknown login attack	**Protection mechanism of unknown login attack**
Use the following regular expression to detect unknown telnet attempt (\\w+ \\d+ \\d+:\\d+:\\d+)(.\\d+: \\w+)(\\d+)(: I SYNRCVD)(\\d+.\\d+.\\d+.\\d+)(:\\d+)(10.0.0.1)(:23) Attackers IP which will be extracted as matcher_variablegroup(5)	**Configure** the following IP ACL Router>en Router#conf t Router(config)#ip access-list standard unknwn_login Router(config-std-nacl)#deny attacker's IP 0.0.0.0 Router(config-std-nacl)#exit Router(config)#interface f1/0 Router (config-if)#ip access-group unknwn_login in

ICMP redirect attack

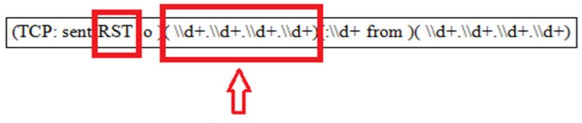
ICMP redirect packets are actually sent by routers to hosts if they find a better path to reach a destination. If a router receives a packet and forwards the packet to the same interface where it had received then an ICMP redirect can be sent. But an attacker can carry a man in middle attack using redirects.

Detection Mechanism of ICMP redirect attack	**Protection mechanism of ICMP redirect attack**
Use the following regular expression to detect ICMP redirect attack	Remove the redirected route from routing table using following command

	**clear IP route destination IP [gateway]** The original (not redirected) route will now be learnt by the router through its running routing protocol.

BGP session termination attack

Tcp reset attack is the attack in which a TCP connection is terminated by the attacker using a spoofed packet with the RST (reset) bit in the TCP packet set. This attack affects BGP protocol.

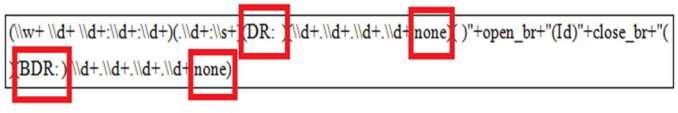
Detection of BGP session termination attack	**Protection mechanism of BGP session termination attack**
Use the following regular expression to detect BGP session termination attack 	Configure the following IP ACL Router>en Router#conf t Router(config)#ip access-list standard unknwn_login Router(config-std-nacl)#deny attacker's IP 0.0.0.0 Router(config-std-nacl)#exit Router(config)#interface f1/0 Router(config-if)#ip access-group unknwn_login in

OSPF hello packet deletion attack

OSPF neighbors exchange hello packets every 10 seconds (Default hello timer is 10 seconds.) When 4 consecutive hello packets are missed by an OSPF process, then the OSPF process declares its neighbor as dead (Default dead timer is 40 seconds.) When a neighbor is dead, its entries will be flushed from the routing table. Attacker can purposely delete OSPF hello packets. After 4 consecutive message deletions, the neighbor ship will break. This is an attack which has caused the OSPF neighborship to break resulting into flushing of its OSPF entries.

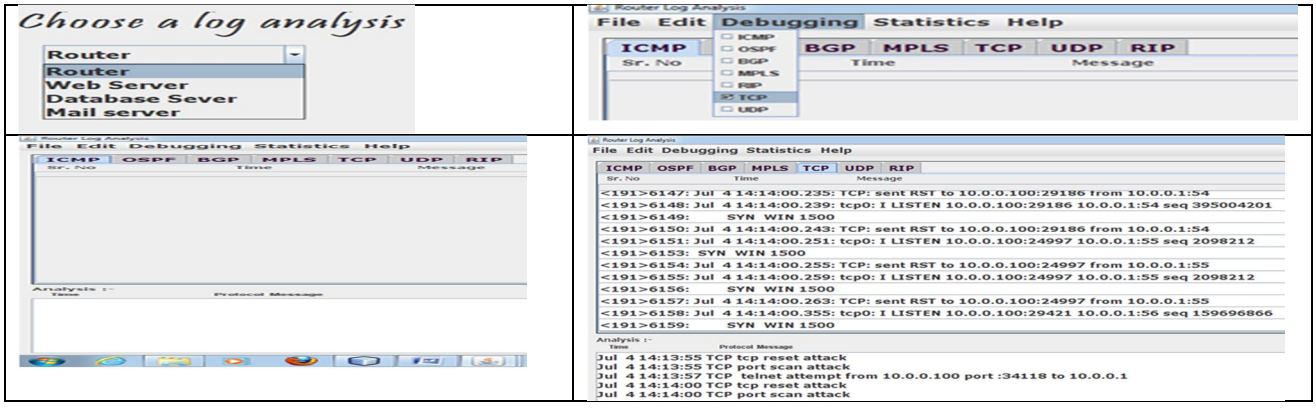
OSPF DR BDR null attack

OSPF is a victim of DR, BDR null attack. OSPF elects DR, BDR on a multi access network. DR, BDR are elected based upon the priority and router ID (highest loopback address) sent in the hello message. After the election is done, the elected DR, BDR are sent in the hello message. An attacker can create a phantom router with highest priority and ID. Attacker will now set DR, BDR to null and then send that hello message. This will force reelection for DR, BDR and will elect the phantom router ad DR which will create undesirable effect.

Detection mechanism of OSPF DR BDR null attack	
Use the following regular expression to detect DR BDR null attack 	open_br=Pattern.quote(open_br); close_br=Pattern.quote(close_br);

Proposed Router IDPS Implementation Results

In this section of this paper is dedicated for actual implementation results and sample output screenshots. Following are the detailed screenshots for:-



Observations from above screenshots are given as below:

- All logs are not mixed. ICMP logs shown in separate tab, After a threshold, an attack alert is shown below
- An ACL is automatically configured on the router after the attack as defense mechanism.
- Attack can happen in absence of the network admin. So ACL is automatically configured to defend the router.

Due to space constraints the screen shots of all the attacks on ICMP, OSPF, BGP, UDP etc. is not simulated. Only attack on TCP is shown herewith.

Conclusions and Future Directions

Router Attacks Detection without log analysis has following problems:

- Several logs were generated having the same time and All logs are intermixed, It's impossible for the network admin who is seeing these logs to detect a DDOS attack. And maybe, by the time he has detected the attack; a huge loss had already occurred.
- Moreover there can be situations when the admin is not present there to see these logs and DDOS attack can happen in his absence.

A complete network security monitoring and management tool which will tell about all the working protocols on the routers, the connectivity between the routers and the malicious activities happening on the routers is not developed till date. This work has created a base and has provided the first step to do so. It has found a way to dump log to separate machine and also sort them. It can fire commands on the router which means it can easily obtain the output of 'sh run' from routers. It knows how to extract information from the log to detect a security attack happened on them. It has also defended routers by configuring adequate ACLs.

References

[1] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks", The Internet Protocol Journal - Volume 7, Number 4, 2004.
[2] "ICMP Attacks Illustrated, SANS Institute InfoSec Reading Room". [Online]. Available: http://www.sans.org/reading_room/whitepapers/threats/icmp-attacks-illustrated_477.
[3] "Routing protocol". [Online]. Available: http://en.wikipedia.org/wiki/Routing_protocol.
[4] Kotikalapudi Sriram, Doug Montgomery, Oliver Borchert, Okhee Kim and D. Richard Kuhn, "Study of BGP Peering Session Attacks and Their Impacts on Routing Performance", IEEE Journal On Selected Areas In Communications: Special Issue On High-Speed Network Security, Vol. 24, No. 10, October 2006.
[5] "Michael Sudkovitch, David I. Roitman,, OSPF Security project book". [Online]. Available: http://webcourse.cs.technion.ac.il/236349/Spring2013/ho/WCFiles/2009-2-ospf-report.pdf.
[6] "Communicate with router". : http:// www. omnisecu. com/ cisco- certified –network –associate - ccna/ how- to- communicate- with- a- router.htm.
[7] "Karsten Iwen, Logging in Cisco IOS".: http://security-planet.de/wp-content/uploads/2008/12/logging-ios.pdf
[8] "Anand Deveriya, An overview of the Syslog protocol, Cisco Press". http://www.ciscopress.com/articles/article.asp?p=426638.
[9] "Cisco IOS Debug Command Reference". [Online]. Available: http://www.cisco.com/en/US/docs/ios-xml/ios/debug/command/s1/db-s1-cr-book.pdf.
[10] "Sean Wilkins, Basic access lists configuration for cisco devices, Cisco Press".: http://www.ciscopress.com/articles/article.asp?p=1697887.
[11] http://www.iss.net/security_center/advice/Intrusions/2000012/default.htm .
[12] Danai Chasaki and Tilman Wolf, "Attacks and Defenses In The Data Plane Of Networks", IEEE Transactions On Dependable And Secure Computing (Tdsc), 2012.
[13] Kirk A.Radley, Steven Cheung, Nicholas Puketza, Biswanath Mukherjee, and Ronald A. Olsson, "Detecting Disruptive Routers: A Distributed Network Monitoring Approach."
[14] Vrizlynn L. L. Thing, Morris Sloman, Naranker Dulay, "Locating Network Domain Entry And Exit Point/Path For Ddos Attack Traffic.
[15] 15. 15. Muhammad Naveed, Shams un Nihar, Mohammad Inayatullah Babar, "Network Intrusion Prevention By Configuring Acls On The Routers, Based On Snort Ids Alerts", Emerging Technologies (ICET), 2010.
[16] sawmill.net - Cisco Systems Router Log Analyzer." , https://www.sawmill.net/for
[17] mats/cisco_router.html., N.p., n.d. Web. 18 Apr. 2017.
[18] White Paper: Automated Analysis of Cisco Log Files.", http://www.networkingunlimited.com/ white007.html. N.p., n.d.Web. 18 Apr. 2017.
[19] Log analysis - Infogalactic: the planetary knowledge core." https://infogalactic.com/info/Log_analysis .N.p., n.d. Web. 18 Apr. 2017.
[20] Saili R. Waichal, Gopal J. Sonune," Router attacks detection through log analysis and defense" IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.3, No3, June 2013.