Intrusion Detection and Prevention System for Routing Protocol Attacks

Kamini Nalavade
Research Scholar, Computer Engineering Department,
VJTI, Matunga, Mumbai,
India

Dr. B. B. Meshram
Professor & Head, Computer Engineering Department,
VJTI, Matunga, Mumbai,
India

***Abstract*—Routing is one of the integral components of any communication network which is responsible for taking routing decision to forward a packet to its destination. Many routing protocols are used for effective routing of network traffic such as BGP, OSPF, EGP, and RIP. Like the other protocols in TCP/IP suite, routing protocols also suffer from severe vulnerabilities. Intruders can exploit these vulnerabilities underlying in routing protocols to affect network communication. It thus becomes necessary to apply some security mechanism to protect them. Objective of this paper is to provide a survey of vulnerabilities and attacks in routing protocols. This paper proposes a model for router intrusion protection and security. Proper analysis of logs can be extremely useful for detecting any anomalous behavior of the router. The aim is to detect any anomalous behavior of packets passing through router which can lead to collapse of entire network using log files of routers. In this paper we give details about how to use router logs for attacks detection and defense. We propose an model for preprocessing and intrusion detection for routing protocols.**

***Keywords*—Intrusion, Security, Vulnerabilities, Router, Log Analysis**

I. Introduction

Today's information systems are distributed and highly interconnected via local area and wide area computer networks. Over time continuous improvement in communication technology have enabled the computer systems on Internet to share and collect information in very less time. The information flow on Internet is constantly under various attacks. The root cause of these exploits is underlying flaws of TCP/IP protocol suite. TCP/IP is a defacto standard of communication on Internet. The intruders spend large part of their efforts and time in finding these vulnerabilities and exploiting them to carry out novel attacks. Routing is an integral part of any communication network. Various routing protocols are used for performing routing in networks such as RIP, BGP, EGP and many more. Vulnerabilities in these protocols is one of the major source of attacks on information flow.

Router is one of the most commonly attacked components in a network. Attackers most of the time attack the router's software and make the router to behave in a malicious way. A router's main core software is the packet processing unit. Nowadays a single router has more than one unit for packet processing to provide faster processing. This processing unit is software which can be compromised by an attacker. So an extra independent hardware is embedded into the router which can do monitoring to detect the software attacks. A typical router with packet processing units looks as shown below:

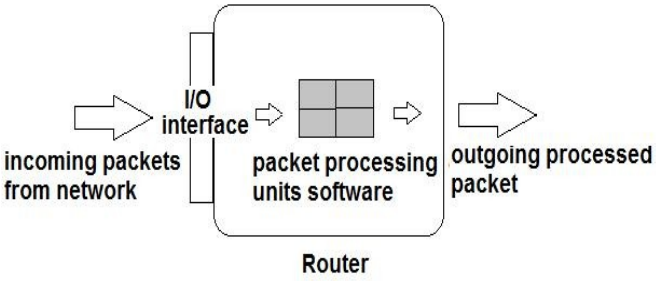


Figure 1. Router with packet processing units

The hardware modules which will do the monitoring will act upon the processing units. The hardware module will learn all the execution paths that can result out of a normal functioning router. If any anomaly is detected then it will detect an attack and drop the current packet and bring the processing unit back to fresh new state. Sometimes just by maintaining a few counters you can find which router is the one who is behaving abnormally in a network [5]. Mostly only 6 counters are enough. For example counter for packets flowing through routers R1 and R2, counters for packets whose source is R1 but which flows through R2. Similarly router a will also maintain three more counters for the opposite direction. We can apply simple rule such as the number of outgoing packets from R1 should be equal to the number of incoming to R2. Same rule can be transformed when some source or destination is involved.

The main objective of this paper to perform intrusion detection and prevention using router log files. The main causes of the intrusions are the underlying vulnerabilities in routing protocols. In Next section we provide a brief overview of vulnerabilities and attacks of routing protocols. In section III our proposed system for routing intrusion detection and protection is discussed. The last section discusses the experiment and results achieved in this area using simulation environment followed by conclusion.

II. Vulnerabilities and Attacks on routing protocols

Routing is the act of moving information across a network. Routing occurs at layer 2 or network layer of the TCP/IP model. Routing algorithms initialize and maintain routing tables which contain route information. The purpose of routing protocols is to learn of available routes that exist on the network, construct routing tables and make routing decisions. There are a number of protocols available for use here. The options available in TCP/IP protocol suite are RIP, IGRP, EIGRP, OSPF,BGP. BGP is the defacto standard for inter-domain communication whereas RIP, IGP, OSPF are the protocols used for intra domain routing.

Vulnerabilities inherent in the design of routing protocols cause many attacks on network. A router can be attacked in many ways by a hacker. Most commonly, Distributed Denial of Service attack like ARP poisoning, Smurf attack, Ping of Death can hit the router that can collapse the entire network. Routing packets between networks is the main aim of a router. Man in the Middle (MiM) attacks can be caused which will direct the traffic to an attacker instead of sending it to the legitimate router. ICMP redirect attack is one such attack. Routers contain routing entries which decide the path selection. Routing entry poisoning is probably the most obvious attack which will make the router to behave in an anomalous way. Vulnerabilities and attacks of some of the major routing protocols are as given below

A. RIP

Currently there are two versions of RIP, RIPv1 and RIPv2. RIPv1 uses broadcast whereas RIPv2 uses multicast. In contrast to RIPv1, RIPv2 supports subnet masks and a simple authentication mechanism. It is UDP-based and stateless. RIP does not use internal sequence numbers. It allows unsolicited route advertisements. In other words, spoofed advertisements are accepted and processed even though no requested it. RIP datagrams are not authenticated. Routing tables can be modified remotely by an attacker. As a result, the target system may be unable to communicate with regular endpoints. Complex 'man-in-the-middle' attacks could also be crafted. Also RIP v.1 understands only classful addressing. The maximum cost allowed in RIP is 16 which mean that the network is unreachable. Thus RIP is inadequate for large networks that is, those in which legitimate hop counts approach 16. RIP does not support variable length subnet masks. There is no facility in a RIP message to specify a subnet mask associated with the IP address and to ensure that routing table updates come from authorized routers. RIP only uses fixed metrics to compare alternative routes. As the size of the routing domain grows, the instability of the vector-distance algorithm in the face of changing topology becomes apparent.

It is trivially easy to spoof RIP. There are no sequence numbers to predict, sessions to hijack, authentication passwords to sniff, trust relationships to spoof, or crypto keys to crack. By spoofing RIP, it is possible to manipulate route tables on routers and hosts. It is also easy to identify RIP-enabled routers and download their route tables by sending them a request message. All routers on a network may be requested via a single UDP broadcast datagram.

B. BGP

The dominant inter-domain routing protocol on the Internet is the Border Gateway Protocol (BGP). The different versions of BGP range from 1–4. BGP has been deployed since the commercialization of the Internet, and version 4 of the protocol has been in wide use for over a decade. BGP enables you to create an IP network free of routing loops among different autonomous systems. BGP can be attacked in many ways. An autonomous system can advertise incorrect information through BGP UPDATE messages passed to routers in neighboring ASes. A malicious Autonomous System(AS) can advertise a prefix originated from another AS and claim that it is the originator, a process known as prefix hijacking. Neighboring As'es receiving this announcement will believe that the malicious AS is the prefix owner and route packets to it. The real originator of the AS will not receive the traffic that is supposed to be bound for it. If the malicious AS chooses to drop all the packets destined to the hijacked addresses, the effect is called a black hole. This attack makes the hijacked addresses unavailable.

Communication between BGP peers can be subjected to active or passive wiretapping. The BGP software, configuration information, or routing databases of a router may be modified or replaced via unauthorized access to a router, or to a server or management workstation from which router software is downloaded. These latter attacks transform routers into hostile insiders, so security measures must address such Byzantine failures. 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. To carry out this attack, the attacker simply sniffs the TCP connection to get the source IP address, source port number, destination IP address, destination port number and most importantly the ongoing sequence number. Now the attacker creates a fake TCP packet with proper source IP and port and destination IP and port. The sequence number is also filled appropriately. The RST bit in this packet is set. When this packet reaches destination, it sees that the RST bit is set and hence it terminates the connection. So the continuity is disrupted until an entire new TCP session is established. This is certainly not desirable.

Man-in-the-middle attack is carried out to intercept the data flowing from a source to a destination. The attacker can simply read the data or even modify the data. Such an attack can be carried out in many ways. One of them is using ICMP redirect packets. 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. The attacker is on the same subnet as the victim. The attacker will send an ICMP redirect which will create a new entry in source's routing table. This entry will have router C as next hop for reaching the actual destination and the attacker successfully intercepts the connection.

C. OSPF

OSPF is a link state Interior Gateway Protocol (IGP) developed for use in Internet Protocol (IP)-based internetworks. It uses cost as its routing metric. A link state database is constructed of the network topology which is identical on all routers in the area. OSPF only provides authentication, not confidentiality. Therefore, hackers can sniff the network for Link State Advertisements (LSA) messages in order to map out the network topology. This is extremely useful information for reconnaissance. Even though OSPF is designed and deployed to be used as an intra- domain routing protocol, in most scenarios and situations an OSPF router will still accept unicast IP packets directly addressed to it. On physical point-to-point networks, the IP destination is always set to the address All OSPF Routers. On all other network types, the majority of OSPF packets are sent as unicasts, i.e., sent directly to the other end of the adjacency. This opens the door to attacks that may be originating from outside the OSPF domain. Timing the stream of different packets needed for a given attack poses a certain degree of difficulty if executed from a remote Autonomous System, but it may not be enough to stop a skilled and motivated attacker.

There are three fields: metrics, sequence number and age which are particularly vulnerable and therefore are the targets of usual attacks. OSPF neighbors are formed by exchanging hello packets. These hello messages are not acknowledged by the other end. When OSPF misses certain hello packets, the neighbor is considered as dead. This depends on dead timer of OSPF. An attacker can purposely delete some OSPF packets. This will cause the neighbor to be declared as dead.

OSPF sends LSAs (Link State Update) to exchange routing information with their neighbors. LSA contains a sequence number which helps the router determine as to which one is the freshest route. An attacker can send LSA containing the max sequence number which is 0x7FFFFFFF. Thus all routers will accept this as the freshest update. This update will stay in the LSDB (Link Sate Database) for one hour thus helping the attacker to harm the network within that period. Apart from these attacks, denial of service is the common attack carried out on routing protocols. Normally a DDoS attack is carried out by scaning to determine vulnerable hosts from where the attack can be carried out. Tools are then installed on these discovered vulnerable systems which can search for other such vulnerable systems and install the tool on them too. This propagation is very fast and forms an army which can cause the DDoS attack on a victim.

III. Proposed Approach for Routing Intrusion Detection and Prevention

Various routing protocols are used for navigating traffic from source to destination in the communication network. These routing protocols play vital role in communication network. But the flaws in these protocols make the communication insecure. Here we try to propose an intrusion protection system to avoid the communication failure. After studying the vulnerabilities and attacks on the routing protocols, routing protocols and security protocols, here we propose a framework for mitigating these attacks. This framework provides intrusion detection as well as intrusion protection for defense-in-depth security.

We have considered Routing Information Protocol (RIP), Border Gateway protocol (BGP) and Open Shortest path First(OSPF) algorithms for our system. The various fields of RIP, BGP and OSPF messages are inspected. The control logic applies traffic accounting; TTL security Check and track of OSPF update messages for security. The proposed system is as shown below.

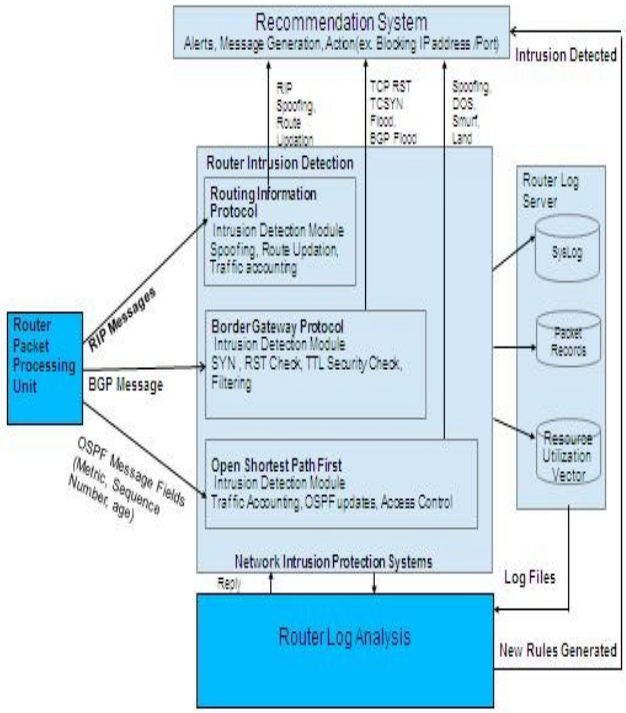


Figure 2 Routing Intrusion Protection Systems

A router's main core software is the packet processing unit. Packet processing unit is responsible for packet capture, packet cleaning and invoking Intrusion detection module. Packet cleaning is the process of removing irrelevant packet fields which are not requied for intrusion detection. Only relevant intrusion detection module will be invoked according to type of routing protocol. Intrusion detection is categorized into RIP intrusion detection, BGP intrusion detection and OSPF intrusion detection to make the attack detection process fast. Intrusion detection module performs the rule matching with header fields of packets. If any anomaly is detected then it will detect an attack and recommendation module will take appropriate action and bring the processing unit back to fresh new state. In routers, many important messages about the functioning and configuration of routers is logged. People often forget of one important in-built intrusion detection system present in almost all network devices which is LOGS. In routers, many important messages about the functioning and configuration of routers is logged. Moreover logs are so huge and their formats are also hard to understand. But if proper logging is

done then one can utilize this LOG facility to detect some attack.

In this proposed system monitoring the separate log files of routing packets is applied as prevention approach. But performing all possible logging causes the router to become slow as lot of logs are generated. In order to use LOGS for intrusion detection efficiently following can be done. As shown in figure 3., the logs are directed to a separate RouterLog Server. Log analysis and processing is performed on a separate machine. One more issue with log analysis is as follows. As huge amounts of logs will be generated every second and it will take a lot of router's physical memory, we dump them to the Log Server.

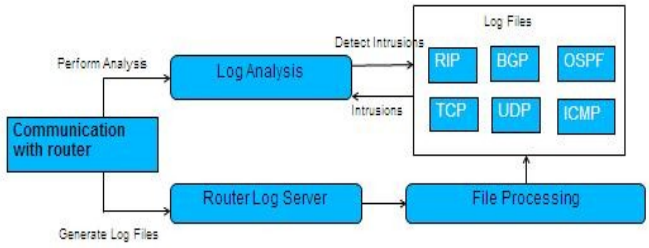


Figure 3 Router Log Analysis

The machine on which the Log server is running is connected to the core switch. In this way, all the routers can direct their logs to the Log server. This gives the network administrator control over monitoring all the routers. Windows doesn't have any built in Syslog facility. You can download Syslog application for windows from the internet. Syslog-ng is the latest with some extra features[5]. To limit the number of messages sent to the Router's Log Server, use the logging trap router configuration command. The logging trap command limits the logging messages sent to RouterLog Servers to logging messages with a level up to and including the specified level argument. The level argument is one of the keywords. To send logging messages to a RouterLog Server, specify its host address with the logging command. The default trap level is informational. The no logging trap command disables logging to RouterLog Server. Kiwi RouterLog Server mentions the source of log entry. It will mention the ip address of router from which the log entry has come. To properly ignore noise from the logs and extract only the useful information requires powerful regular expression matching mechanism. Java provides a lot of classes for regular expression. In our model, we have used class Pattern and class Matcher extensively.

IV. Experimentation and Results

Our proposed system is implemented with following system configuration and results are also discussed.

1. Router Configuration:

One can communicate with a router using any of the following ways [4]

• Using Console port: Router has a console port. A console cable can connect your machine to the router. A terminal emulator program like hyperterminal or putty is required on your machine. This will give you access to the router prompt.

• Using Aux port: By using a remote computer through a modem that calls another modem connected to the router with a cable using the Auxiliary Port on the router.

• Using protocols: Protocols like Telnet, ssh, http, https can be used to connect to the router over a network.

In our system, we are going to use telnet connection to communicate with the router. Line vty on router needs to configured to achieve telnet connection. The RouterLog Server is a machine which will have an ip address. Suppose it is 10.0.0.1. Router has a command which is "logging ip_address" where the ip_address is an argument. It's the ip address of the RouterLog server machine. Use this command to direct all the logs to the Server

Router(config)# logging 10.0.0.1

A router can log information to console, host (syslog), snmp, buffer, monitor (ssh, telnet). Logging to console can be turned OFF if it is ON [6]. In our system, we want to direct logs to another host (RouterLog Server).

2. Router's Log Server

Log files generated by the router are huge and will require large space to store data. We want to store all the logs for analysis. A different system is dedicated which can act as a Log Server. It has memory in its hard disk. Minimum 80 gb of hard disk space will be enough. It's easy to manage that space. All the logs from the router will be directed to this Log Server. Kiwi syslog server can be used on Windows System. The algorithm for implementing Log Server is given below

Algorithm: RouterLog

Server Input: Packet P

Output: Log Files

Step1: Oper UDPPort 514 on the system where IPAddress=ServerIPAddress

Step2: Receive Packets where port=514 && IPAddress=ServerIPAddress

Step3: Separate Header & Data from

Packet Step4: Write Data part in a file

Step 5: End

So now the logs are successfully stored on the Routerlog server. This also provides a clean separation. The router console will not be interrupted with logs now. The logs can be viewed on the separate machine. Log analysis can now be done on this machine. Log server will be continuously

running. Along with Log server, few other modules will be deployed on the system.

```
May 13 22:40:09.455: OSPF: Send hello to 224.0.0.5 area
0 on FastEthernet1/0 from 10.0.0.1
```

Figure 4 Sample Log entry

As one can see, every entry has month, date, time, protocol, log message. We will extract the protocol field through regular expression matching in java. Based on the protocol, the log entries will be written to different file as shown in Fig 3. Fig 3. shows that 6 different files were created: TCP, UDP, ICMP, RIP, OSPF, BGP as we want to detect attacks protocol wise. For example, OSPF attacks will be different from TCP and so on.

3. Intrusion Detection

This section will focus on various attacks and how these intrusion will be detected successfully by the system. This is the main aim for router log analysis: Intrusion 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:

3.1 OSPF hello packet deletion attack: OSPF neighbors exchange hello packets every 10 seconds. When 4 consecutive hello packets are missed by an OSPF process, then the OSPF process declares its neighbor as dead. 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 deletion, the neighborship will break. To generate log entry for each OSPF hello packet sent or received, the 'debug ip ospf events' debugging command can be used. This will enable logging for OSPF events. The log entry for the hello packet is as shown in Fig. 4 The Hello packet attack detection algorithm is given below:

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 match occurs, copy *seconds_time* into *init_hello_time*.
4. Create an array *times* of size 6 of all possible seconds_time.
5. Match every new hello log entry *seconds_time* with *times[i]*. If the values are not equal then
    a. Calculate number of hello missed using modular arithmetic method within the *times* array.

3.2 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. When a port scan happens on a router, the log entries which are generated are shown in Fig. 5

```
May 14 10:58:25.627: tcp0: I LISTEN 10.0.0.100:1495
10.0.0.1:1 seq 1473192529

May 14 10:58:25.791: tcp0: I LISTEN 10.0.0.100:1496
10.0.0.1:2 seq 4232257361

May 14 10:58:25.883: tcp0: I LISTEN 10.0.0.100:1497
10.0.0.1:3 seq 452016969
```

Figure 5 Port Scan Attack Detection

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 algorithm for detecting port scan attack is as given below:

Input: Source & Destination IP

output: port scan atack detection

1. Search in the log for matching TCP listen entry
2. If the pattern is matched
    1. Extract time field in t
    2. if flag==0
        1. start counter=0
        2. Set timestamp=t
        3. Set flag=1
3. else
    1. increment the counter
4. if counter>=threshold and display ==0
    1. print port scan attack
    2. Set dispaly=1
5. if current time= timestamp+120sec
    1. Set flag==0 && display==0

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.

3.3 ICMP redirect attack

The log entry after an ICMP redirect attack, BGP session termination attack is given in Fig. 6

```
May 13 23:25:07.938: ICMP: redirect sent to 10.0.0.1 for
dest 172.16.1.111 use gw 172.21.80.23

May 13 22:48:42.515: TCP: sent RST to 10.0.0.100:100
from 10.0.0.1:
```

Figure 6 ICMP redirect Attack Detection

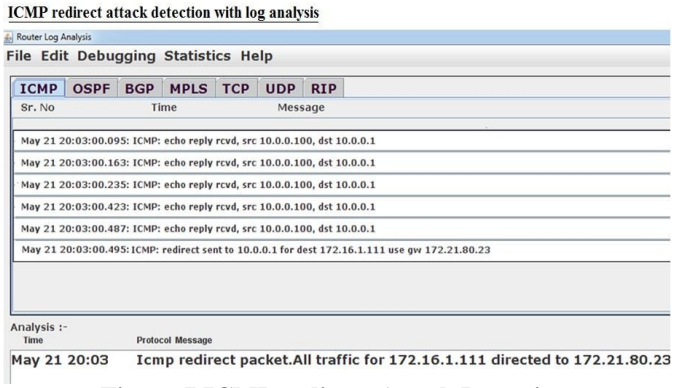


Figure 7 ICMP redirect Attack Detection

In our system we could successfully detect the redirect attack on ICMP as shown in figure7.

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. The log entry after telnet attempt is shown in Fig. 8

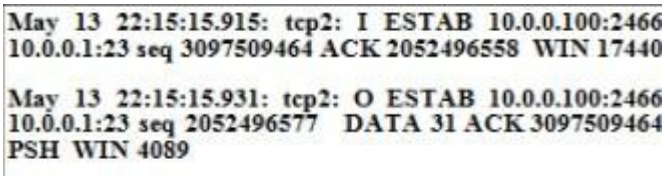


Figure 8 Router accessed using telnet

3.4 OSPF DR/BDR Attacks

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 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 compromised 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 comporomised router. The raw log after a DR, BDR null attack is shown in Fig. 9

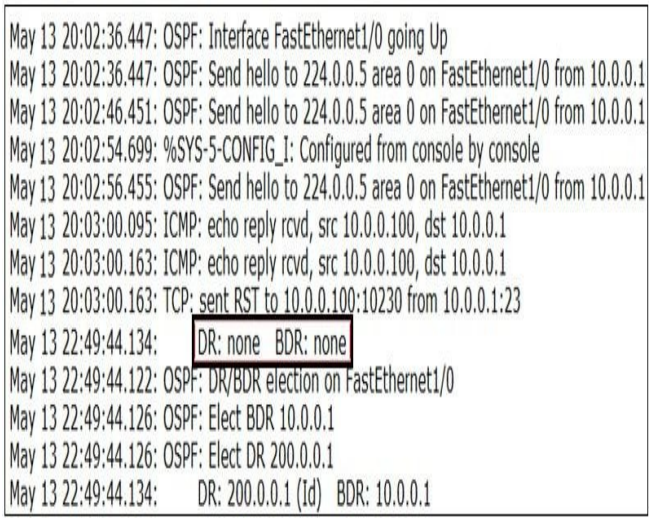
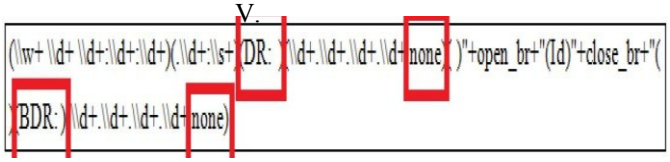


Figure 9 Router log entry for DR/BDR values

Use the following regular expression to detect DR BDR null attack.

V.



Conclusion

The design flaws of TCP/IP routing protocols have been responsible for most of the attacks on the Internet. Different types of attacks are targeted towards the router.This paper has presented various vulnerabilities & attacks directed at TCP/IP routing protocols and focused on intrusion detection. Various security mechanisms are devised to protect the router from such attacks. Log analysis can also be one such method for router security. But the logs that are sent over the network use the UDP (user datagram protocol). UDP is not reliable. Hence some log packets can be lost. Also the log formats might change for different IOS (Cisco's Internetwork Operation System). Thus automated log analysis can help us remove all the noise from the logs and actually concentrate on only the important entries for network management and security. In our proposed system, we try to evaluate routing attack targeed at BGP, RIP and OSPF.

References

[1] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraк, DISTRIBUTED DENIAL OF SERVICE ATTACKS, The Internet Protocol Journal - Volume 7, Number 4, 2004.

[2] ICMP Attacks Illustrated, SANS Institute InfoSec Reading Room

[3] Michael Sudkovitch and David I. Roitman, OSPF Security project book, 2010.

[4] Danai Chasaki and Tilman Wolf, ATTACKS AND DEFENSES IN THE DATA PLANE OF NETWORKS, IEEE transactions on dependable and secure computing (tdsc), 2012.

[5] Kirk A.Radley, Steven Cheung, Nicholas Puketza, Biswanath Mukherjee, and Ronald A. Olsson, DETECTING DISRUPTIVE ROUTERS: A DISTRIBUTED NETWORK MONITORING APPROACH.

[6] Vrizlynn L. L. Thing, Morris Sloman, Naranker Dulay, LOCATING NETWORK DOMAIN ENTRY AND EXIT POINT/PATH FOR DDOS ATTACK TRAFFIC.

[7] 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.

[8] Anand Deveriya, An overview of the Syslog protocol, Cisco Press, 2005.

[9] Karsten Iwen, Logging in Cisco IOS.

[10] Sean Wilkins, Basic access lists configuration for cisco devices, Cisco Press, 2011.

[11] Cisco IOS Debug Command Reference, Release 12.3.

