Router Attacks-Detection And Defense Mechanisms

Saili Waichal, B.B.Meshram

Abstract: Router is one of the most important components of any network. Their main aim is taking routing decision to forward a packet to its destination. It can be a home or small office router which takes your traffic on the internet; or it can also be one of the core routers which form the backbone of the internet. Being such an important component, routers are often targeted for attacks. It thus becomes necessary to apply some kind of security mechanism to protect them. This paper gives a survey of different methods for router management and security. The aim is to detect any anomalous behavior of router which can lead to collapse of entire network. It then focuses on using an excellent in built feature available in almost any machine like router or web server or mail server or switch or database server which is LOGS!!! Proper analysis of logs that are generated can be extremely useful for detecting any anomalous behavior of the router. Thus logs can provide us huge information for solving a misconfiguration on router or detect an intrusion on the system. In this paper we give details about how to use router logs for attacks detection and defense.

Index Terms: Access Control lists, Regular Expression Matching, Router Attacks, Router Debugging, Router Logs, Router Security, Syslog.

1 Introduction

Routers are one of the most important devices in a network. A router can be compromised in many ways by an attacker. Section II gives an overview of many such attacks on routers. Many tools have been built to protect routers. Section III focuses on many such security mechanisms developed to detect and defend such attacks. It can be a hardware module independent from the router or can be a software solution by using Snort and ACLs. Then we propose a system where the router logs can actually be used to detect and defend such attacks.

2 Types for Router Attacks

2.1 Distributed Denial of Service Attack [1]

Denial of Service attack causes a victim to be denied of service that he requests. When this attack is caused by a host on a network it is called Denial of Service attack whereas if the attack is caused by a group of people over networks together then it is called Distributed Denial of Service attack. Normally a DDoS attack is carried out by the attacker/attackers in following way:

1. Scans are carried out to determine vulnerable hosts from where the attack can be carried out. Vulnerable systems can be one where there is no antivirus running or whose antivirus is not updated.
2. Tools are then installed on these discovered vulnerable systems which can carry out the attack. After installing these tools, these vulnerable hosts also search for other such vulnerable systems and install the tool on them too. This propagation is very fast and it quickly forms an army which can cause the DDoS attack on a victim.

Some of the DDoS attacks that can happen on a router are as follows:

1. ARP (Address Resolution Protocol) poisoning: Here the attacker continuously looks for ARP request packet in the network. Once it finds a request packet, it quickly forms a packet with a wrong MAC address and sends it as reply. So a wrong mapping will take place in ARP table which is referred to as ARP poisoning. So now the actual MAC will be denied of any further service.
2. Ping of Death: Here the attacker forms a packet containing more than 65536 bytes. IP protocol cannot handle packets with size more than 65536. So when such a packet is received, it leads to undesirable effects on the victim's machine.
3. Smurf attack: Here the attacker sends out a lot of ICMP echo request packets to different hosts. The source address of all these echo request packets is kept as the address of the victim by the attacker. Now the victim gets flooded with ICMP echo reply packets. Thus the victim can't process important stuff because it gets busy in processing the echo reply messages.

2.2 Man in the Middle Attack

Here the attacker manages to intercept the data flowing from a source to a destination. The attacker can simply read the data or even modify the data.

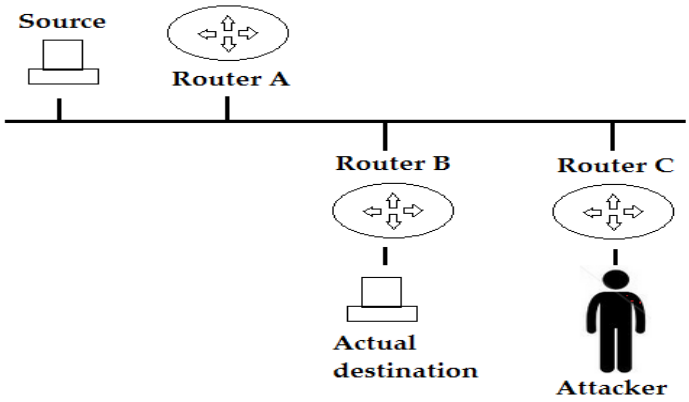

Fig. 1 ICMP redirect attack

- *Ms Saili Waichal is currently pursuing masters degree program in Computer Engineering and IT in VJTI, Mumbai, India. E-mail: saili.waichal@gmail.com*
- *Dr. B.B.Meshram is Head and Asst. Professor, Dept. of Computer Engineering and IT. E-mail: bbmeshram@vjti.org.in*

Such an attack can be carried out in many ways. One of them is using – ICMP redirect for a router [2]. 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. In Fig. 1, 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. So here the attacker successfully intercepted the connection.

2.3 Tcp Reset 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. 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. The severity of this attack varies from application to application. For example, Cisco's BGP protocol is highly affected by this attack. BGP is the protocol that runs in the service provider architecture and has to manage huge routing tables. Whenever a route goes down, BGP does a lot of processing over many routers to fix the problem. In this case if the tcp attack is carried out, bgp will do a lot of processing because of the terminated connection. If a connection is terminated frequently, bgp also gradually isolates that router from the network because it is held responsible for causing a lot of processing frequently over many routers. So a harmless router can be isolated because of such an attack.

2.4 Attacks on OSPF [3]

1. Hello packets dropped: OSPF neighbors are formed by exchanging hello packets. These hello 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.
2. Max Sequence attack: 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.
3. Attacking external routes: Routes that come from external areas or autonomous systems are trusted. Such routes are not checked for validity. So an attacker can send false external routes which will not be validated.

2.4 Unknown Logins

Attackers who do not have direct physical access to a router can crack the routers telnet password and log into the router and reconfigure it which can make the router act maliciously.

3 Security Mechanisms

A lot of research work has been done in the area of network management. Router is one of the most commonly attacked components in a network. So a lot of network management work focuses on monitoring behavior of routers. In this survey, we aim to summarize a few notable works in this area. Attackers most of the time attack the router's software and make the router to behave in a malicious way. The attackers target the software. Even if you try to detect the malicious activity by another software, there may be fair chances that the monitoring software is also successfully compromised by the attacker. To overcome this problem, hardware based monitoring was done [4]. A router's main core software is the packet processing unit. Nowadays a single router has more than one unit for packet processing. This facilitates faster processing. This processing unit is complete 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. The hardware obviously wont be compromised by the attacks meant for the software. Now a typical router with packet processing units looks as shown below:

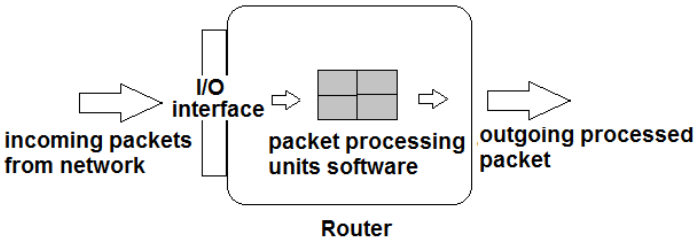

Fig 2. Router with processing units

The hardware modules which will do the monitoring will act upon the processing units.

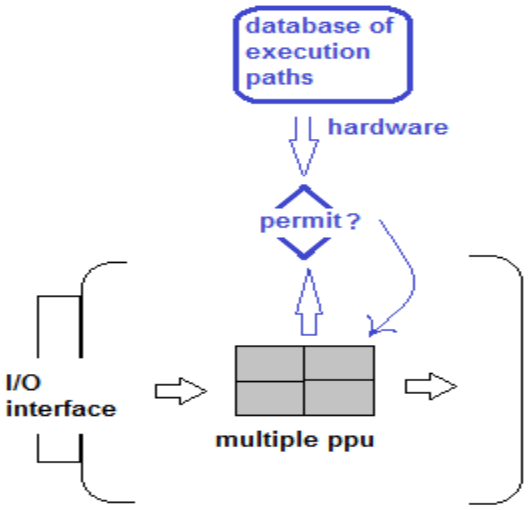

Fig 3. Hardware monitoring module

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.

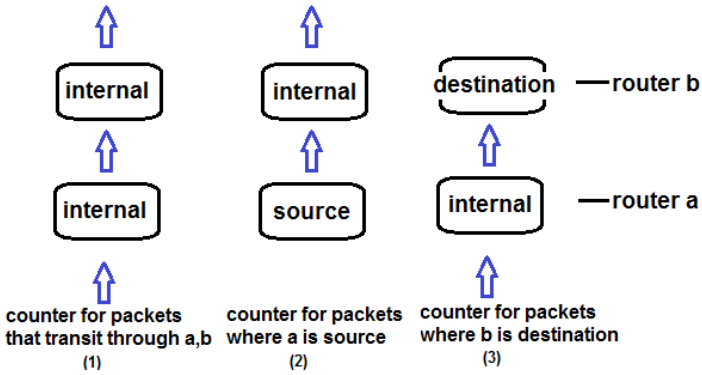

Fig 4. Counters maintained by router

Fig. 4 shows three counters which will be maintained by router a

1. A counter for packets that flow “through” both a, b
2. A counter for packets whose source is a but which flows through b
3. A counter for packets that flow “through” a but whose destination is b

Similarly router a will also maintain three more counters for the opposite direction. Now by simply using a rule which says that the number of packets (consider size) that are outgoing from a should be equal to the number of packets that are incoming to b. This is the rule when both a, b are internal routers. Same rule can be transformed when some source or destination is involved. In networks, DDoS (Distributed Denial-of-Service) is the most popular attack. Moreover it is the attack where the router doesn’t behave abnormally. It just receives too many packets for processing. So the router spends all its resources in processing the packets and drops the legitimate packets that really needed attention. Packets that flow through the network are routed based on the destination field. The source field is not verified to check whether it is a legitimate one or one which is forged. So an attacker can easily forge thousands of ip addresses and fire packets to a router destination. Now it was observed that the routing table doesn’t change drastically very often. So a packet with a certain source and a certain destination will flow through a certain path according to the routing table. The routers can learn such paths over time. So now if a source address is forged, then router will detect the unusual path that was taken for that source and destination. So a router can systematically learn ip address that it forwards. It can maintain this as the permitted list of ip addresses. Suddenly when the router sees huge traffic, it can stop learning the ip addresses and drop only those packets which are not there in the permitted list till the attack is under control [6] Snort can also be used to detect any intrusion in router and also took measures to take action for that intrusion using ACLs(Access Control Lists) [7]. Snort is an open source tool which works as an IDS (Intrusion Detection System). Rules are written in Snort and they are matched against the packets. An example of a rule is as follows

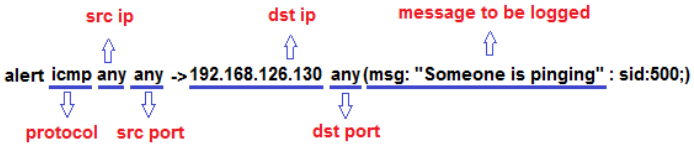

Figure 5. A snort rule

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. Snort is an open source tool and is easily available. Access control lists is an in built feature in routers and very powerful when security is concerned. So the router is secured with very less cost overhead.

4 Proposed System

Above section focused on various network management and security mechanisms. Now we propose a new system which can also do router monitoring. 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. But turning ON all possible logging causes the router to become slow because a lot of logs are generated. So this feature is often ignored because they don’t want to compromise on the speed of the router. 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 any misconfiguration or detect some attack. In order to use LOGS for intrusion detection efficiently following can be done

4.1 Syslog Server

4.1.1 Size

The biggest problem with logs is its huge size. Routers have very less memory to store the huge logs. When the memory is small, the logs get overwritten. The newer logs replace the older ones very fast because huge logs are created per second. We certainly don't want this to happen. We want to store all the logs for analysis. This can be achieved from a separate Syslog server [8]. A different system is dedicated which can act as a Syslog Server. It has memory in its hard disk. Minimum 80 gb of hard disk space will be enough. Its easy to manage that space. All the logs from the router will be directed to this syslog server. Kiwi syslog server can be used on Windows System. Following commands will direct all the logs to the Syslog Server

- First you will turn ON all the necessary logging (Turning ON all possible logging is not recommended because it will make the router slow)
- The Syslog 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 Syslog server machine. Use this command to direct all the logs to the Syslog Server Router(config)# logging 10.0.0.1

4.1.2 Separation

So now the logs are directed to a separate Syslog server. This also feels like a clean separation. You can do entire log analysis and processing on a completely separate machine away from the router.

4.1.3. Logging Levels

One more issue with log analysis is as follows. The logs are often very huge. If all possible logging is turned ON, then it will seriously impact the normal functioning of the router. Huge amounts of logs will be generated every second and it will take a lot of router's physical memory to display or dump them to the Syslog Server.

Levels: There are eight different logging levels [9]. To limit the number of messages sent to the syslog servers, use the logging trap router configuration command. The full syntax of this command follows: logging trap level The logging trap command limits the logging messages sent to syslog 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 syslog server, specify its host address with the logging command. The default trap level is informational. The no logging trap command disables logging to syslog server.

4.2 Log analysing program

Now a syslog server is built. The syslog server can be for a single router or multiple routers can also share the same syslog server. Kiwi syslog server mentions the source of log entry. It will mention the ip address of router from which the log entry has come. Now the analyzing program will have the following modules

4.2.1. Regular expression matching

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. Both the classes are available since java version 1.4. For example, following is simple example for extracting an ip address:-

```
Pattern ip_addressp = Pattern.compile ("(\\d+.\\d+.\\d+.\\d+);

Matcher ip_addressm = ip_addressp.matcher (line);

if (ip_addressm.find())
{
        // do something
}
```

Fig 6. Extracting ip address

4.2.2. Communication with router

Once an attack or a misconfiguration is detected, some defense mechanism should be taken to curb it. Access lists are an excellent tool for router security. So according to the anomalous behavior of the router, appropriate access lists should get configured on the software through the program. So there should be a way to fire commands onto the router from the program. This can be achieved by Java's strong network programming. Thus communication is done with the router using java's Socket class and various reader and writer classes like BufferedReader and PrintWriter. Using BufferedReader, all the output from the router can be read. Based on that, the write method of PrintWriter will write appropriate commands on the router.

This communication will help achieve the following:-

1. It will help to configure appropriate access lists on the router as a defense mechanism [10].
2. Turning ON all possible logging slows down the router. So it will be used to turn ON only needed logging via debugging commands [11].

4.2.3. Deployment of the program

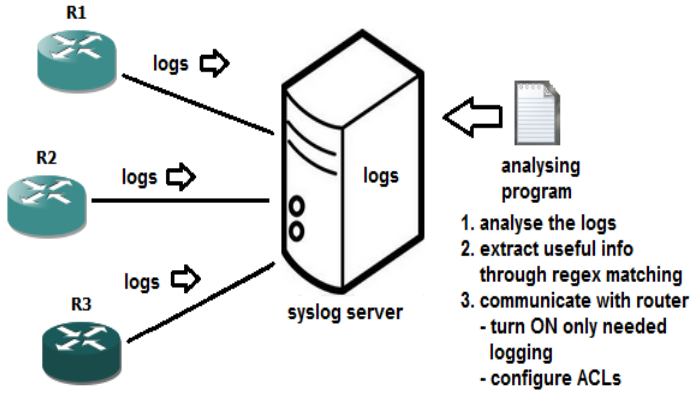

Fig. 7 Deployment of analyzing program

It will be appropriate to deploy this program on the same system where the syslog server is running. So this analyzing program will have local access to the syslog file.

5 CONCLUSION

Different types of attacks are targeted towards the router. 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. Some mechanisms can be done to prevent loss from such failure. Also the log formats might change for different IOS (Cisco's Internetwork Operation System). So a way can be found to deal with these changes also. 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.

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

[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.