INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Snort Rule Technique For Detecting Worm Attacks

J. Viba Mary
Assistant Professor, Department Of Computer Science
St. Paul's College Of Arts & Science For Women, Tamil Nadu, India
P. Gayathri Devi
Assistant Professor, Department Of Computer Science,
St. Paul's College Of Arts & Science For Women, Tamil Nadu, India

Abstract:
All over the world, the computerization gets increases and it is really hard task to provide security for the systems connected to the network. In 1988, Morris worm proved that, it can bring the internet down in hours which lead to large queuing delays and high packet loss. So the security of networking will make us to prevent all the confidential data to be maintained safely without any loss. Amongst the various security risks, worm attack is the most severe attack threat, that can be easily self replicated and uses a network to send copies of itself to other end terminals on the network without any user intervention. To avoid such attacks, a technique called Snort rules is proposed to secure the network. It will detect the worms by analyzing the probable paths where they tend to copy themselves. As a summary, the paper shows that Snort rules technique is faster in detecting any kind of worms and provide full authentication to the network.

Key words: *Worms, self-propagating security, Internet worm detection*

1.Introduction

Nowadays many software companies are using one or more systems to handle their projects in an effective way of connecting through Local Area Network (LAN). The connection is mainly for file sharing, communication, work sharing, and common file access etc. So the deletion of common file or spreading of an unwanted message can be done easily by an unauthorized person by using a LAN connection. This is due to lack of security. There are many types of attacks like Trojan horse, Worms and Viruses, etc.

The most challenged topic which are still under research for a recovery solution is the worm attack. A worm is a small program that can reproduce itself. It can spread the copy of itself to other computers. Worms are serious security threat, which may cause congestion in the network. If a small worm happens to attack a terminal system in the network, it starts to launch a crypto viral attack, delete files, disrupt network traffic services and attack email networks for various purposes. It takes very less time to complete its task. Once the system is affected, it immediately gains control over the system and start replicating itself. The user doesn't know even that worm has taken control over the whole system. Within no time the entire network goes out of control from the users and gets all the confidential file or information to be destroyed.

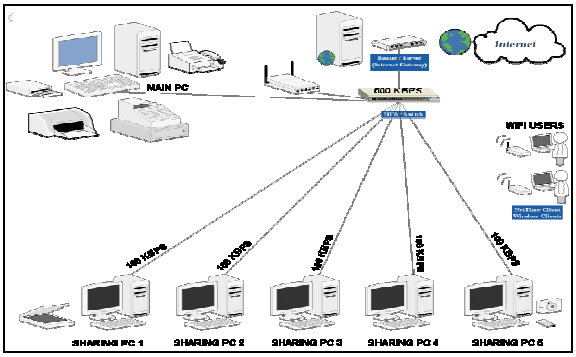

Figure 1

In this paper, a new solution is used to ensure the security of the systems connected in network. Here the time is taken under consideration to complete the process. The goal of this study is to detect the worms or any malicious behaviour that can cause any vulnerability, by using a special technique called Snort Rules. If any, such a worm exists, and then automatically it is detected and deleted. If an infectious packet is found to be transferring over the network, it will be discarded.
The rest of the paper is organized as follows. In section 2, the details of the related work are presented. In section 3, the overview of the worm is mentioned. In section 4, the types of worms are explained. In section 5, the Snort Rule technique is implemented. In section 6, the performance of Snort Rule technique is analysed. In section 7, the future enhancement is discussed and in the last section 8, the paper is concluded.

2.Related Work

In 2000, the I LOVE YOU [3] worm had affected a million of computers in the world wide. It spreads through e-mail with the subject of "I LOVE YOU", and an attachment "LOVE-LETTER-FOR-YOU". Upon opening the attachment, the worm reproduces itself by sending a copy to everyone in the windows address book.
In 2001, Darrel [1] Showed that epidemic style attacks have been occurred by spreading Code red [4] and Nimda [1] worms. Once the internet is broken down, it will cause a huge economic loss. There are some solutions to solve the worm attack. One of the solutions is updating antivirus, but it cannot detect the unknown worms. The other solution is using firewalls and routers, it can block the worm traffic signature but this occurs after the worm spread.
Yang et al developed an algorithm for worm detection. It has two sub algorithms. They are short term and long term algorithm. In the first algorithm it can detect the worm and in the second algorithm it can detect only at certain types of worms. Moreover in that paper, it focused only for detecting the worm type's attacks and there is no determination of equations.
The above related works are mainly focused on detecting various attacks caused by worms and uses various techniques to avoid the worm attack. In this article, the Snort Rule technique is proposed. This type of technique is mainly used to examine, detect and report the results. In addition, it can detect any kind of malicious behavior or worms if exist in any system in the network and stop them from spreading all over the network.

3.Overview Of Worms

Worm is a self-propagate or self-replicate malware that can spreads over a network of computers. It can able to propagate through a network without any human intervention like a virus; a worm is also a small program which can replicate itself. If any network is infected by a worm, then immediately worm starts to reproduce itself, spread to other computers, delete files on the infected systems, launch a crypto viral attack, and disrupt network services for various purposes. The worm is not an executable program.

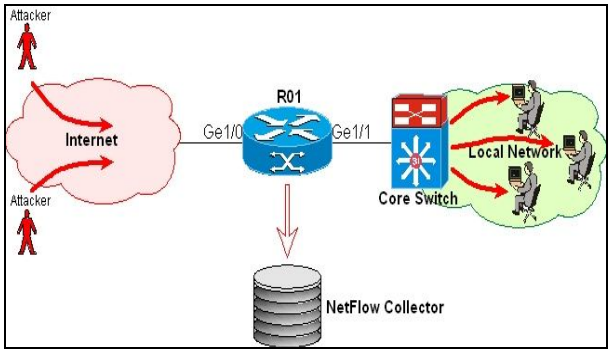

Figure 2

4.Types Of Worms

In this section, the worms can be classified into several forms as follows.

- Email worm
- Instant messaging worms
- Internet worms
- IRC worms
- File sharing network worms.

4.1.E-mail worm

The worm can be easily spread via e-mail messages. If once the form of attachment is opened, the next second the infected messages may contain a link to an infected website. Then it starts propagating itself without any intervention. The best way to infect other computer in the network is only done by using e-mail communication.

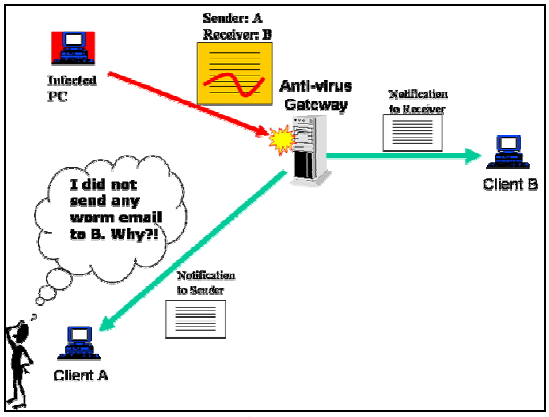

Figure 3

Known methods to spread are

- Ms outlook services
- Direct connection to SMTP servers using their own SMTP API.
- Windows MAPI functions.

Some of the e-mail worms are

- VBs/Love letter@MM,
- W32/Nimala. gen@MM, M32 Mydoom. f@MM, etc..

4.2.Instant Messaging Worm

The instant messaging worms can be spread via any instant messaging applications like email worm. The instant messaging worm also will send links to an infected websites on the local contact list. The only difference between these two worms is the way chosen to send the link. Eg. W32/yahlover. worm.

4.3.Internet Worms

Using the local operating system services, the worm can scan the entire feasible path that is connected to network resources for vulnerable machines. It will attempt to connect these machines, so that it gains full control over the network. If any machines are not patched, the worm scans the internet machines still open for exploitation. Request will be sent which install the worm downloader. If it happens then the worm will execute and start infected. Some are w32/Nimdagen@MM, w32/codered. f. worm, etc.

4.4.IRC worms

IRC (Internet Relay chat) uses the same technique like instant messaging worms to propagate. Eg. VBS/loveletter@MM, w32/pandem. worm etc.

4.5.File Sharing Network Worms

For file transferring, common internet file system (CIFs) protocol was designed to share files in confidential but there is a loophole that can reflect the worm attacks. Eg. W32/mydoom.f@MM, w32/pandem.worm.

4.6.Characteristics Of Worms

- Without any intervention [2] of an administrator it deletes all the files in the hardware.
- Changes all the settings.
- The system gets slow and the process becomes very hard.
- It can spread itself through instant messaging, mails etc., using a compromised machine.
- Software error will occur, so that the software will not get open, software gets hanged or it will be closed without any reason.
- The private information a data will be disclosed to the hacker.

5.Methodology

5.1.SNORT Tool

SNORT is an open source network intrusion prevention system which can perform real-time traffic analyzing and packet logging on IP network. Snort rules are a simple, lightweight, flexible and powerful language. In version 1.8, the Snort rules [11] were written in a single line but in current, it may use a multiple lines by adding a backslash to the end of the line. It has two sections. They are rule header and rule options. In the 1st section it contains the protocol address and information of both the source and destination rules and net masks. In the 2nd section, it contains alert messages and information where the parts of the packet should be inspected to determine if the rule action should be taken.

It can be able to perform content searching and matching, which is used to detect the different kinds of attacks, and protocol analysis. It can be used as a packet logger, packet sniffer or full blown and network intrusion prevention system.

- Packet sniffer mode:
  It reads the packet of the network and displays on the screen like a TCP dump.
- Packed logger mode:
  It logs the packets to disk for anomalous activity.
- Network intrusion prevention system mode:
  It analyzes the network traffic for matches and performs malfunctions.
- Inline mode:
  It obtains the packets from IP tables, and then causes it to drop on Snort rules.

5.2.SNORT Plug-Ins

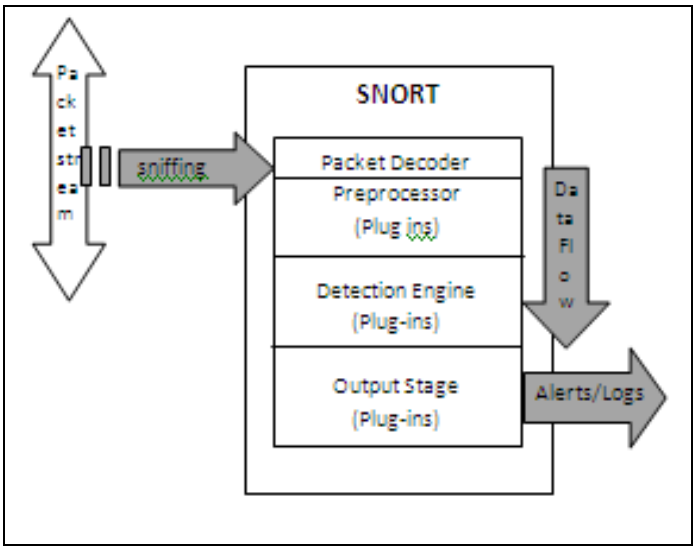

Figure 4

- Preprocessor:
  The packets are examined and analyzed before it is processed.
- Detection:
  It can perform a simple test on each packet one by one.
- Output:
  Report the results.

5.3.Implementation

In this proposed work, the entire work is divided into two modules. In the first module, the database is maintained which contains all the types of possible existence worms along with the locations. Then the detection code is made to run on all the systems, in order to check whether there are any worms are existent in the location. If so, then the detected worm will be deleted and discarded simultaneously. But there is a possibility, where the detected worms will not be in the locations that are stored in the databases. In such cases, the second module is performed, ie it analyzes the packet data. It compares the content in the packet and data content by using Snort rules. Since the Snort rules which contain the data will detect that whether the data in the packet which is transferred over the network is infectious packet or not. Thus at the end of these two modules, the system is secured from various attacks like virus, worms and infectious packet data.

6.Performance Analysis

The performance is analyzed by using scalability and time factor.

6.1.Scalability

In this article, the scalability is unlimited i.e. the worm detection algorithm code is installed on only one system and not to all over the network. This leads to increase the scalability to be more. The code is to connect to multiple systems. It can be used for n number of systems without any connection.

6.2.Time factor

In the project, the code is made to run, and then it takes around 2 sec for the execution.
eg. No. of locations traversed and searched for worm =35
Time taken for location traversed = 2sec
Time taken for each location = 2/35 sec = 0.057 sec

There are two modules. In the 1st module, the database is maintained by the information of worms that exist today. Now the system should free from those worms.

In the second module, the data in the content are compared to the packet data in the network with Snort intrusion detection system rules to detect whether the packet is infectious or not. By using Snort rules, there are 37 rule files to be matched with the packet content. For this, we take 10 packets to test the performance.
No. of Snort rule file considered =37
No. of packets considered for each run=10.

For each retrieval, it may take approximately 30 Sec, because it needs to combine data retrievals. The time may be reduced, if the number of packets is considered at a time or taking main Snort rules like FTP, TFTP deleted rules etc. So the time taken depending on the hardware configuration of the system.

7.Future Enhancement

The future LAN network will need to be more adaptive and optimizing continuously the use of its resources and recovery from various attacks, faults and transient problems. As part of our future work, the basic Snort rule technique can be applied even in a Wide Area Network to provide full authentication and to be highly secure. In this paper we have maintained a database to detect the existing worms and discarded. The same technique can be quite elaborated for the future projects i.e., the database with the worm information's can be updated when, new locations of worm are known. In future, if any, better detection system is introduced, that can also be used in this project which would yield better results.

8.Conclusion

It is necessary to detect the worms and provide full authentication to the system over the network. For this, we maintained the database with worm's information. By using the database the infected worms are identified and deleted. If the worms which are not presented in the database, we have implemented the second module, which can compare the data content and packet data using the NIDS and deleted the worms and discarded. Thus, the results show that the NIDS detects the worm faster than other algorithms. It can also detect different types of worms and give secured transmission of shared files between the source and destination all over the network.

9.References

1. Darrel M.Kienzle, Mathew C.Elder,"Recent worms: A survey and Trends".Worm '03 proceedinfs of the 2003 ACM workshop on Rapid malcode.
2. Lemos, R."year of the worm: Fast spreading code is weapon of choice for Net vandals".CNET News.com,Http://news.com/2009-1001-254061.html,March 2001
3. "I LOVE YOU" WhoWhatWhereWhenWhy.com-Retrived 2008-05-26.
4. Moore, David: Collen Shannon(2001) ' The spread of the Code-Red Worm(CRv2)" CAIDA Analysis.
5. Thomas chen, Jean-Marc Robert(2004)." The evolution of viruses and worms". Retrieved 2009-02-16, Northcutt.S(2002) Network Intrusion Detection, New Riders publishers.
6. Sourcefire Inc.,Roesch.M, and Green.C,(2000) "SNORT users manual-SNORT Release:2.6.0", Available at:http://www.SNORT.org.
7. Vishrut Sharma, IEEE, "An Analytical survey of Recent Worm Attacks", IJCSNS, voL.11. No.11, Nov 2011.
8. http://virusall.com/computer%20 worms/worms.php.
9. Symantec Security Response. http://www.symantec.com/Security-response.
10. ThreatExpert. http://www.threatexpert.com.
11. Y.V. Srinivasa Murthy & et.al., "A Noval Approach to Troubleshoot Security Attacks in Local Area Networks", IJCSNS, VOL.11, No.9. September 2011.