Trend Analysis of Snort Alarms

K.Chantawut and B.V.Ghita

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Network intrusions have been active topic for researches for many years. However, in order to gain insight into the nature of the current threat on the Internet is challenging. This paper, addresses this problem by systematically analysing a set of traffic trace collected over three months in front of the firewall at the Internet gateway of the University of Plymouth. The motivation of this study is to quantitatively understand the nature of the current Internet threat which leads to long-term analyses of trends and the recurring patterns of attacks. In the study, fundamental features of intrusions activities was investigated by evaluating the log data along a number of aspects (e.g. daily volume of intrusion attempts, the source and destination of the intrusion attempts and specific type of intrusion attempts, etc.). The result of the study shows both a large quantity and wide variety of intrusion attempts. It also shows that numerous amount of denial of service and ICMP scanning activities can be detected as common threats on the Internet. The patterns of these activities can be found at daily timescale and the on/off patterns exhibit recurrence of correlated behaviours. Furthermore, worms like SLAMMER and Sasser.D still persist on the Internet long after their original release. Deeper investigation reveals that sources of intrusions spread all over the globe. However, a major proportion of intrusions are from China. Also a very small proportion of sources were responsible for a significant portion of intrusion attempts for a given period of time.

Keywords

Trend analysis, Intrusion detection system, Snort, DoS, SLAMMER

1 Introduction

Prevention is normally recognized as the best strategy to protect critical information infrastructure from malicious attacks. Security staffs or network administrators must understand the trend of the threats in order to be able to prevent any catastrophic damage to their networks in advance. The understanding of the trend of the attacks would help organisations to determine the current fitness of their security systems and the budget for improving the system to defense against cyber attacks due to the uncertainty of the occurrence of the attacks.

Even though, currently, there are various tools to help analysing intrusion data, for example, BASE (Basic Analysis of Security Engine), SnortSnarf. These tools provide querying and presenting the intrusion analysis in easy to use graphical mode. However, the tools offer only basic and limited set of analytic options to users. It is not possible to perform in depth statistical analysis using these tools, for instance, to

look for the trends of attacks from specific country or to forecast the trend in the future. This is the initiative why this study was conducted.

Instead, the research has involved obtaining and anonymising the traffic traces coming toward the university as the inputs to the IDS, then extracting and analysing the output of the IDS to gain an understanding of the behaviours of the threats (e.g. the source countries, number of attacks per unique IP, the distribution of attack on the targets) and be able to analyse the nature of some of major threats using normal statistic and time series analysis theories.

2 Related Studies

The trend analysis of network attacks is an important subject in IDS. Many of related studies have been focused in the field of the analysis of Internet intrusion trends. Many of the studies are based on packet level investigation of intrusion logs generated by either firewalls or IDS.

The well known projects existing on the Internet that have been set up to collect large scale attack data from firewall and intrusion detection logs are the SANS Internet Strom Center and Symantec's Deep Sight system.

(Moore, 2004) provides the analysis that gives a better understanding of the nature and the long term trend and recurring patterns of the denial-of-service (DoS) attacks on the Internet. The study concludes that DoS attacks are a common threat for those depending on the Internet.

The study of (Yegneswaran, 2003) investigates fundamental features of intrusions activities by evaluating the log data along a number of dimensions (e.g. daily volume of intrusion attempts, the source and destination of the intrusion attempts and specific type of intrusion attempts, etc.).

The studies of (Jouni, 2009; Kim, 2007; Wu, 2005) focus on finding best-fit forecasting model for the studies of anomaly detection analysis. (Wu, 2005; Jouni, 2009) present various types modeling techniques based on time series analysis for representing the dynamic of intrusion and attack activities including the comparison of the model accuracy.

3 Common Intrusions

3.1 Viruses and Worms

Typically, viruses are attached to excusable files and they need human interaction to infect target hosts. A virus may only exist on a computer and it cannot be spread without a human action, by sharing infecting files or sending e-mails with viruses.

A worm is similar to a virus by its design. However, it has the ability to copy itself from machine to machine through computer networks. A worm takes advantage of known vulnerabilities in software or the operating system. The infected computer

could send out hundreds or thousands of copies of itself. The end result is that the worm uses up computer time and network bandwidth causing service outage.

3.2 Scanning

The purpose of scanning is to collect as much information as possible about target networks or hosts using tools to send probes into targeted systems and listen to the response which is coming back. At the end, if it is successful, attackers will gain information about vulnerabilities and openings (i.e. ports or services or live hosts) of victim's networks.

4 Network based Intrusion Detection System (NIDS)

NIDS monitors the traffic in specific network segment or subnet. NIDS looks for anomalies in the traffic, such as port scanning or denial of service attacks. In order for NIDS to be effective, it has to be located where it can monitor the most traffic that an organization deems critical. Therefore, placement is critical to the success of uncovering of anomalous traffic or behaviour in the monitored area.

There are, typically, two types of detection mechanisms using by NIDS which are **"signatures (or rules) based detection"** and **"anomaly based detection"**. In signature based detection, the NIDS look in bytes codes and expressions to match any known attacks expressions (signatures or rules). When it matches any intrusion, flags an alarm. Signature based detection is useful for detect known threats but it cannot detect new unknown threats or even the variants of already defined attacks.

In anomaly based detection the NIDS first establishes a normal activity model (a baseline) after training the system for specific period of time. Then the NIDS will use the baseline model to detect suspicious events that deviate from normal activity model. If an anomaly is detected, the will flag alerts for an intrusion. The benefit of anomaly detection is that it can detect unknown threats without having to understand the cause of the threats. The main problem for this approach is that it is prone to false alarms.

Snort is the most famous open-source intrusion detection system capable of performing packet logging and analyzing real-time traffic on computer networks.

5 Time Series Analysis

In general, the analysis of a time series will be based on the fact that observations close together in time will be more closely related than observations further apart and values in a series for a given time will be expressed as deriving in some way from past values, rather than from future values.

5.1 Stationary Time Series

In stationary time series, the random variables fluctuate about a fixed mean level, with constant variance over the observational period. This property is a requirement

for time series analysis because there must be a sort of regularity exists in the time series so that the behaviour of the time series can be predicted. Various levels of stationarity exist; however, in a context of univariate time series, the time series must satisfy the assumption of **"weakly stationary",** that the mean is a constant, independent of any time shift.

5.2 Autocorrelation (ACF)

ACF is a statistical measure that captures the correlation between different time shift samples (or lag) of the process. (NIST/SEMATECH, 2006) has summarised the main purposes of ACF into two points. The first purpose is to detect the non-randomness in time series and the other is to identify an appropriate time series model if the data are not random.

5.3 Long Range Dependency (LRD) and Self Similarity (SS)

A stationary process is said to be "Long Range Dependence (LRD)" if it has a high degree of correlation between distantly separated data points, even across large time shifts. Whereas in short range dependence processes, the correlation between values at different times decreases rapidly as the time difference (lag) increases.

"Self Similarity (SS)" is a property of an object whose appearance remains unchanged regardless of scale of which it is viewed. Self similarity detected in the intrusion data could explain certain characteristics and behaviours of a specific intrusion attempt. It is also useful to note that some self-similar processes may exhibit LRD, but not all processes have LRD are self-similar. The degree of SS and LRD can be estimated by the calculation of "Hurst parameter (H)". For a self-similar process with LRD, the value of H will be in the range of $0.5 < H < 1$. As $H \rightarrow 1$, the degree of both self-similar and LRD increases. Any pure random processes would have $H = 0.5$.

6 Examining Snort Alarms

6.1 Data Collection

The data for this study was collected from the Internet gateway of the University of Plymouth network. The collection used a SPAN port of a layer-2 switch located in front of the university's firewall to capture traffic. The reason for this is to ensure that the overall behaviour of Internet attacks on internal network can be studied; otherwise the firewall would filter out most of the attacks before the traffic is captured. The purpose of the study was not to test the efficiency of the university firewall, but to observe the amounts, structure, and evolution in time of the alarms.

Capturing network traffic on high speed network requires very large storage. Therefore, in order to overcome this problem, Snort, running in packet logger mode, was utilised to capture only header parts of the network traffic. The filter was set to capture only the traffic destine to the internal subnet of the University of Plymouth

(UoP) network. The traffic traces were collected from 24/04/2009 to 28/07/2009 period.

Due to user privacy and network security concerns, the destination IP addresses of traces (i.e. the IP addresses within the university) had to be anonymised in prefix-preserving way prior to the analysis, so that the traces would still contain the structure of the subnet. More details on the anonymisation tools used and the associated procedure can be found in (Koukis, 2006; Foukarakis, 2007)

Then the next step was to analyse the released anonymised traces using snort. For this study, Snort (version 2.8.4.1 and VRT Certified Rules released on 21/07/09) was run in off-line mode to detect alerts in the captured traffic traces using signature based detection method. As the large amount of traffic traces were analysed, the unified alert record format was set as the output in the snort.conf because of the small size and the completeness of details contained in the output.

Subsequent to successfully creating the complete unified alerts, Barnyard was used to convert all the unified alert files generated by snort into a single output file in ***csv*** format.

6.2 Distribution of Alerts

There were totally 71 types of alerts, distinguished by unique Snort's signature ID (SID), detected by Snort which contributed the total number of 157747024 alerts. Only 3 types of alerts, which are triggered by Snort Signature IDs (SID) 2003, 2004, 2050 represent almost 95% of all the attacks. It was found that these alarms were all represent the MS-SQL (SLAMMER) worm attacks and generated by the same packets and similar snort rules. Therefore, the duplicated alarms were removed and the distribution of SLAMMER alerts is plotted in Figure 2.

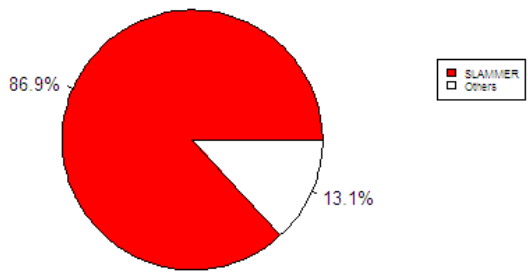

Figure 2: Distribution of SLAMMER attacks

Nevertheless, even the duplicates were removed, the proportion of SLAMMER is still very large (87%) compared to the others. The next figure shows the distribution of other alerts after removing SLAMMER.

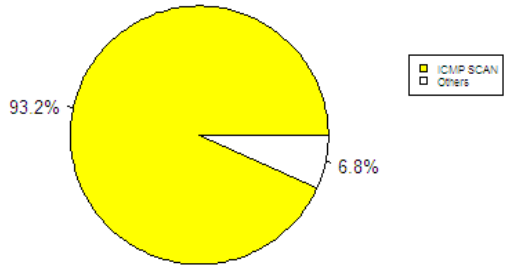

Figure 3: Distribution of ICMP Scanning attacks

After removing SLAMMER, it was found that there were another 3 types of ICMP scanning attacks presented as the majority in the alarms, which were ICMP NMAP PING (SID469), ICMP L3retriver (SID466) and ICMP PING CyberKit (SID463). All these scanning attacks represented 93% of the rest of the alarms.

From the above analysis, it can be said that the majority of intrusion attempts on the Internet were governed by SLAMMER and ICMP scanning attacks. Therefore, the trend analyses were based on SID2003 to study the trend of SLAMMER and SID469 to study the trend of ICMP scanning. The results of the study would represent the trend of the majority of the attacks on the Internet.

6.3 Analysis of SLAMMER

The analysis of SLAMMER attacks showed that the attacks came from all over the World (i.e. 125 countries). However, the majority were from only top five countries which were China, Korea, the United States, Romania and Mexico. China was the main contributor of SLAMMER attacks and all the top attacking hosts were all in this country. The analysis also showed that the majority of SLAMMER attacks on the Internet were governed by only small clusters of hosts each automatically and constantly broadcasting a vast number of the worms and the number of attacks did not necessarily depend on the number of the attacking hosts. Additionally, it was found that the periodic pattern of attacks in every 24 hour might cause by the competition for Internet bandwidth among the SLAMMER sources and the packet drop by SPAN port overloading during peak hours. There was no specific target of the attacks as the number of attacks on each unique IP was normally distributed all over class B of the University of Plymouth's allocated space. The analysis of the time series of number of the attacks per hour showed that the time series was nonstationary, however, strong degree of correlation and periodicity could be spotted from the ACF plot which supported by further analysis on Self Similarity (SS) and Long Range Dependence (LRD) by the calculation of Hurst parameter. The results showed strong degree of SS and LRD exist in the time series.

6.4 Analysis of ICMP NMAP PING

The analysis of ICMP NMAP PING also showed that the attacks came from various part of the World (i.e. 75 countries) and the United Stated was the largest source of the attacks. The results of the analysis showed that ICMP NMAP PING had similar

behaviours to SLAMMER worm attacks in the ways that most of the major attacks seemed to be automatically generated processes, came from a small group of hosts and this type of attack also had a periodic pattern of 24 hours. As a matter of fact, it could be the target discovery part of Sasser.D worm attack as mentioned in (Hideshima, 2006). The daily pattern of attacks was also found. It was spotted that the volume of attacks tended to very active during the peak hours when the most number of targets were active. The targets of ICMP NMAP PING were also as diverse as the targets of SLAMMER. However, it was found that the targets were focused on only 12 IP hosts which received the most number of attacks. The analysis of the time series of number of ICMP NMAP PING per hour showed that the time series was also nonstationary with strong degree of correlation and periodicity. Further analysis on the time series was done to find the degree of Self Similarity (SS) and Long Range Dependence (LRD) by the calculation of Hurst parameter. The results showed strong degree of SS and LRD exist in the time series.

7 Comparison of the results to previous studies

The analysis shows the similar finding as the two prior studies (Moore, 2004; Yegneswaran, 2003) in the way that DoS activities are numerous, a very small collection of sources are responsible for a significant fraction of intrusion attempts and there is a little sign of reduction of such intrusion attempts. This could mean that the behaviour of intrusion attempts on the Internet, especially DoS attacks, has not been changed very much since the earlier studies of the attacks and the situation tends to be going on as common threats on the Internet for very long period of time.

8 Conclusion

The results of the analyses of the can be summarised into the following points:

- Numerous amount of denial of service and ICMP scanning activities could be detected as common threats on the Internet.
- A detection of continuous pattern of ICMP scanning activities could be an indication of a victim discovery phase of another worm (DoS) attack.
- Worms like SLAMMER and Sasser.D still persist on the Internet long after their original release.
- China has now become the largest distributor in injecting attacks onto the Internet.
- A large number of attacks were generated by a small number of attacking hosts.
- DoS and information gathering attacks showed the behaviours of being automatically generated attacks sent by the infected hosts as the daily patterns of these attacks could be detected throughout the observation period.

9 Recommendations

Two recommendations can be made for future study. Firstly, in order to obtained accurate collection of alarm records and, hence, the meaningful analysis results, Snort must be updated and optimised before the analysis begins.

Secondly, to obtain more complete collection of data to be analysed, the problem of packet being dropped before reaching the sensor must be mitigated by implementing a network TAP to capture the flow of traffic to the sensor instead of using SPAN port.

10 References

Hideshima, Y. and Koike, H. (2006). STARMINE : A Visualization System for Cyber Attacks. In Proc. *Asia Pacific Symposium on Information Visualisation (APVIS2006)*, Tokyo, Japan. CRPIT, 60. Misue, K., Sugiyama, K. and Tanaka, J., Eds. ACS. 131-138.

Jouni, V., Herv, D., Ludovic, M., Anssi, L. and Mika, T. (2009) Processing intrusion detection alert aggregates with time series modeling. *Information Fusion,* 10**,** 312-324.

Kim, D., Lee, T., Jung, D., In, P. H. and Lee, H. J. (2007) Cyber Threat Trend Analysis Model Using HMM. *Information Assurance and Security, International Symposium on*, The Third International Symposium on Information Assurance and Security.

Koukis, D., et al., (2006) A Generic Anonymyzation Framework for Network Traffic. *Communications, 2006. ICC '06. ,* 5**,** 2302-2309.

NIST/SEMATECH (2006) e-Handbook of Statistical Methods. The National Institute of Standards and Technology (NIST), http://www.itl.nist.gov/div898/handbook/eda/section3/eda35c.htm (Accessed on 30/06/09).

Wu, Q. and Shao, Z (2005) Network Anomaly Detection Using Time Series Analysis. *Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services.* IEEE Computer Society.

Yegneswaran, V., Barford, P. and Ullrich, J. (2003) Internet intrusions: global characteristics and prevalence. *Proceedings of the 2003 ACM SIGMETRICS international Conference on Measurement and Modeling of Computer Systems.* San Diego, CA, USA, ACM.