

國立交通大學

理學院應用科技學程

碩士論文

網路安全監控行為之實作與分析



**MONITORING AND BEHAVIOR ANALYSIS OF  
NETWORK SECURITY SYSTEMS**

研究生：劉明輝

指導教授：蔡文賢 教授

**中華民國九十六年十二月**

網路安全監控行為之實作與分析

**MONITORING AND BEHAVIOR ANALYSIS OF NETWORK  
SECURITY SYSTEMS**

研究生：劉明輝

Student : Ming-Hui Liu

指導教授：蔡文賢

Advisor : Wen-Hsien Tsai

國立交通大學  
理學院應用科技學程  
碩士論文



Submitted to Degree Program of Applied Science and Technology  
College of Science

National Chiao Tung University  
in partial Fulfillment of the Requirements  
for the Degree of  
Master  
in

Degree Program of Applied Science and Technology

December 2006

Hsinchu, Taiwan, Republic of China

中華民國九十六年十二月

# 網路安全監控行為之實作與分析

學生：劉明輝

指導教授：蔡文賢

國立交通大學理學院應用科技學程碩士班

## 摘 要

隨著電子商務及網際網路的普及，故網路的安全問題也受到重視，然而分散阻絕服務 (Denial of Service) 的攻擊不僅一般的網站無法解決，就連知名的網路大站也同樣無法抵擋，其攻擊者彈指間的動作，往往令企業損失甚重；而世界各國的資訊戰也不斷的上演，足以了解資訊安全所帶來的影響之大。



本論文將以 NIDS Snort 為例實作與分析網路攻擊行為之程序，並將入侵事件記錄分級後，利用不同的記錄等級將來源 IP address 標示成可疑、威脅、惡意等三個狀態存放在 IP 狀態資料庫中，最後以不同的記錄分級與 IP address 狀態來提供網管人員不同重要層次的記錄資料，以減輕記錄過多的問題。

關鍵詞：入侵偵測系統、分散式阻絕服務攻擊、網路安全。

# **MONITORING AND BEHAVIOR ANALYSIS OF NETWORK SECURITY SYSTEMS**

Student : Ming-Hui Liu

Advisors : Dr. Wen-Hsien Tsai

**Degree Program of Applied Science and Technology**

**National Chiao Tung University**

## **ABSTRACT**

As the E-Commerce and the internet become popular, people pay much more attention to the security issues of internet. However, Denial of Service attacks cannot be solved by ordinary websites; nor did by the famous ones. Usually, just in a second, it caused enterprises lost a lot. Moreover, information warfare is fiercer around the world. Therefore, people know that information security plays a big role.

This thesis will take NIDS Snort as an example to analyze the procedure of network attacks. The records will also be stored in IP status database by 3 kinds of IP address sources which marked in doubtful, baleful, and spiteful. Finally, by different record categories and IP address status, MIS staff can focus on the important ones among the huge records.

Keywords: Intrusion Detecting System; Denial of Service attacks; Network Security

## 誌 謝

在碩士專班這幾年學習的過程中，令人倍感珍惜，當然也要感謝家人和親愛的太太瀨云之體諒與配合；在歷經研究學習過程之後，終於完成這篇論文，也許稱不上對學術有所貢獻，但培養出訓練自己發現問題，與尋找解答的能力。老師教學熱忱嚴謹，且對學問一絲不苟的態度，更是學生所要學習的。個人力量太小，而受人之惠太多，謹將本論文獻給曾經幫過我的所有人。



劉明輝 謹識

九十六年十二月

# Contents

---

## **CHAPTER 1 INTRODUCTION 1**

<b>1.1 THESIS MOTIVATION</b> .....	1
<b>1.2 THESIS CONTRIBUTION</b> .....	2
<b>1.3 THESIS ORGANIZATION</b> .....	2

## **CHAPTER 2 BASIC CONCEPT OF DOS AND IDS..... 3**

<b>2.1 DENIAL OF SERVICE (DoS) &amp; DISTRIBUTED DENIAL OF SERVICE (DDoS)</b> .....	3
2.1.1 <i>The DoS attacks</i> .....	3
2.1.2 <i>The DDoS attacks</i> .....	3
<b>2.2 INTRUSION DETECTION SYSTEM (IDS)</b> .....	6
<b>2.3 IDS SNORT</b> .....	8
2.3.1 <i>Snort Rules</i> .....	10
2.3.2 <i>Rule Tree</i> .....	14
2.3.3 <i>Preprocessors</i> .....	15
2.3.4 <i>Variables</i> .....	15
2.3.5 <i>Weakness</i> .....	16
2.3.6 <i>Snortlog analysis tool</i> .....	16

## **CHAPTER 3 IP STATUS DATABASE ..... 18**

<b>3.1 INTRUSION BEHAVIOR ANALYSIS</b> .....	18
<b>3.2 DIVIDING THE RULES INTO URGENCY LEVELS</b> .....	20
<b>3.3 BUILD IP STATUS DATABASE</b> .....	21
<b>3.4 RECORDS ANALYSIS</b> .....	23

## **CHAPTER 4 SNORT LOG ANALYSIS..... 28**

<b>4.1 TESTS ENVIRONMENT</b> .....	28
<b>4.3 TESTS RESULT</b> .....	34

## **CHAPTER 5 CONCLUSION ..... 38**

## **REFERENCE..... 39**

# *List of Figures*

---

FIGURE 2-1 DDoS LAYER CONTROL.....	4
FIGURE 2-2 DDoS ATTACKING-STAGE 1 .....	5
FIGURE 2-3 DDoS ATTACKING-STAGE 2 .....	5
FIGURE 2-4 DDoS ATTACKING-STAGE 3 .....	6
FIGURE 2-5 HOST-BASED IDS .....	7
FIGURE 2-6 IDS DEPLOYMENT DIAGRAM.....	7
FIGURE 2-7 NETWORKS-BASED IDS .....	8
FIGURE 2-8 SNORT STRUCTURE.....	9
FIGURE 2-9 TCP HEADINGS .....	12
FIGURE 2-10 SNORT RULE TREE STRUCTURE.....	15
FIGURE 3-1 BAD IP FINITE STATE.....	21
FIGURE 3-2 CONFIGURATION OF RECORDS ANALYSIS SYSTEM .....	27
FIGURE 4-1 SNORT RECORD ANALYSIS SYSTEM .....	28
FIGURE 4-2 PICTURE OF RULE GRADE SETTING .....	29
FIGURE 4-3 PICTURE THAT RULE SHOWED BY ITS TYPE.....	29
FIGURE 4-4 PICTURE THAT RULE SHOWED BY ITS LEVEL.....	30
FIGURE 4-5 PICTURE OF SOURCE IP ADDRESS PLACING .....	30
FIGURE 4-6 PICTURE OF RELATED IP RECORDS .....	31
FIGURE 4-7 RECORDS ANALYSIS TABLE.....	31
FIGURE 4-8 RECORDS ANALYSIS EXAMPLE—THE RECORDS THOSE ARE EMERGENCY AND THREATENING IP ABOVE.....	32
FIGURE 4-9 REAL TIME SURVEILLANCE .....	33
FIGURE 4-10 RECORD ANALYSIS QUANTITY STATISTICS TABLE AFTER 30 DAYS. 36	
FIGURE 4-11 RECORD ANALYSIS QUANTITY STATISTICS TABLE AFTER 40 DAYS. 36	
FIGURE 4-12 RECORD ANALYSIS QUANTITY STATISTICS TABLE AFTER 50 DAYS. 37	

# *List of Tables*

---

TABLE 3-1 RECORDS ANALYSIS TABLE.....	24
TABLE 3-2 RECORD ANALYSIS QUANTITY STATISTICS TABLE .....	25
TABLE 4-1 SIZE OF SNORTS RECORDS FILE .....	34
TABLE 4-2 COMPARISON WITH USING RECORD ANALYSIS SYSTEM AND ORIGINAL RECORDS.....	37





# CHAPTER 1

## INTRODUCTION

### 1.1 Thesis Motivation

Due to the upsurge of internet and E-Commerce, popular websites face many problems, like the solutions of the bandwidth, powerful server and server cluster. However, it seems that the supply of bandwidth and computer processing speed will never catch up the demand. Taking chance of the limited resources, the attacker, and hacker launch Denial of Service (DoS). In February 2000, the attacks which made internet service unavailable for few hours caused two billion US dollars loss from related revenue; market capital loss and security maintain expenses. Because the attacks were through internet, it cost not much and the risk is also low due to the law problems among different countries.

In fact, information security is the responsibility of all the human beings. Often, the hackers hide themselves to invent being tracked by changing their ID and attack indirectly. Therefore, they first will intrude the systems with less security protection, such as personal computer and school computers. Generally speaking, the benefit from investing the establishment of network security is not easily measured. It seems the same results between no attacks without guard and successfully block with guard. Moreover, usually the blocking only increase the difficulty of being attacked and reduce the loss. If the attacks don't cause actual loss, ex. Leak of data or loss from transaction stop temporarily of E-commerce websites, normally, internet security issue is not the top concern. We hope that we can take internet security seriously and don't become the assistant of hackers. Maybe it doesn't cause loss to the host via DDoS attack, but it made the host becomes the weapon provider of the attacker and harms those being attacked.

## 1.2 Thesis Contribution

Currently, many researches can not provide effective solutions for the DDoS. In fact, the effective way can be started from each host. As long as each computer is with security protection, the DDoS can't work successfully. Therefore, we will introduce the DDoS, analyze its operation principle, and list out the current solutions. In the meantime, for the problem of overwhelmed records from rule-based Intrusion Detection System (IDS), we will take Snort as an example to decrease the problems by analyzing records and making them readable.

## 1.3 Thesis Organization

Below is the content of following chapters:

In Chapter 1, we will discuss the DDoS attacks and the current methods for defense. In Chapter 2, we will introduce the internet-based intrusion detection system that becomes more and more emphasized with Snort example as the illustration. In Chapter 3, we will illustrate the IP status database that build upon the basis of attacking behavior and it's application in records analyzing to reduce the Snort overwhelmed records problem. In Chapter 4, we will introduce the practical system and analyze the result of the experiments. In Chapter 5, we will make a conclusion for the researches of this thesis.

# CHAPTER 2

## BASIC CONCEPT OF DoS AND IDS

### 2.1 Denial of Service (DoS) & Distributed Denial of Service (DDoS)

#### 2.1.1 The DoS attacks

DoS (Denial of Service) is just like that you build a store for customer shopping. The attackers interrupt customer shopping at your store by occupying your store or line up at the entrance. When it happens, the store cannot provide the service in time. For example, web provider cannot provide the website service; ftp server cannot provide files uploading and downloading; email service cannot able to be sent and received.

DoS attacks were often used while sending mass of fault IP address packets at the same time so that the server being attacked cannot afford ( i.e. over the capacity ) or over the maximum linked quantity to paralyze the internet or server so that end user cannot get the service of the server.

#### 2.1.2 The DDoS attacks

Because DoS attacks are via sending faulty mass packet from one point, we can find the attacker from a simple flow surveillance system (i.e. MRTG that often used by TANET). To avoid the disadvantage and get better effect of DoS attacks, the hackers change the original pure DoS attacks to multi-tier and develop them as multi-points ( as figure 2-1 ). Therefore, by screening the statistics of the flow surveillance system, we can only narrow down the attacked areas to a limited IP addresses range. However, when we find these IP address,

most of them are only a relay. The real hacker may possibly be behind many relays. Moreover, as the packet IP address is faulty, it's very difficult to trace back the attackers from IP address.

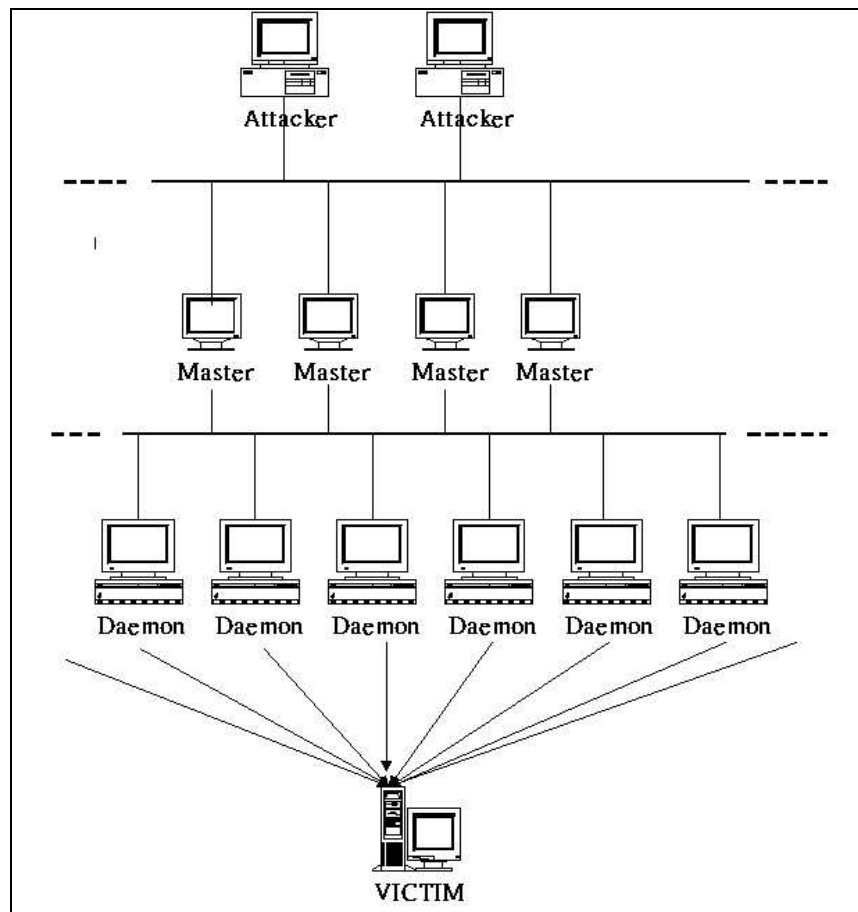


Figure 2-1 DDoS Layer Control

Attacker; Master: Control Side

Daemon: Program Side; Victim: The host which is attacked

DDoS (Distributed Denial of Service) attacks are via a main terminal to control many distributed hosts those have been attacked. While receiving the command of attacking, it will send mass packets to target computers. The target computers cannot work when the flow is overwhelming. The so-called "Distributed" Denial of Service is because it attacks distributed computers. The attacking flow is as below:

A. Hackers intrude hosts then install software which is with specific function (ex. Enable to send mass faulty packets or scan the weak points of the internet automatically); like figure 2-2.

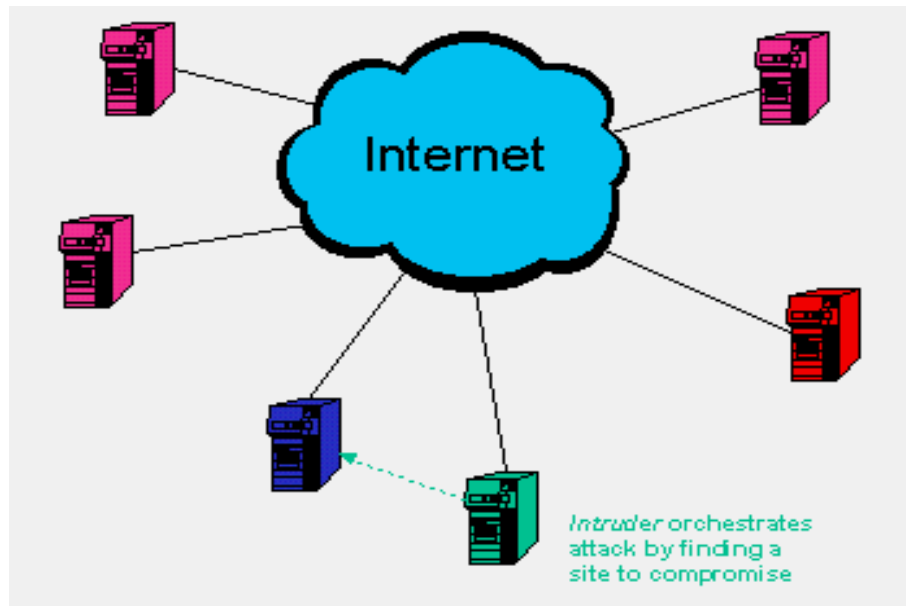


Figure 2-2 DDoS Attacking-Stage 1

( Figure Source [11] )

B. The hackers can intrude more hosts through the attacked hosts; like Figure 2-3.

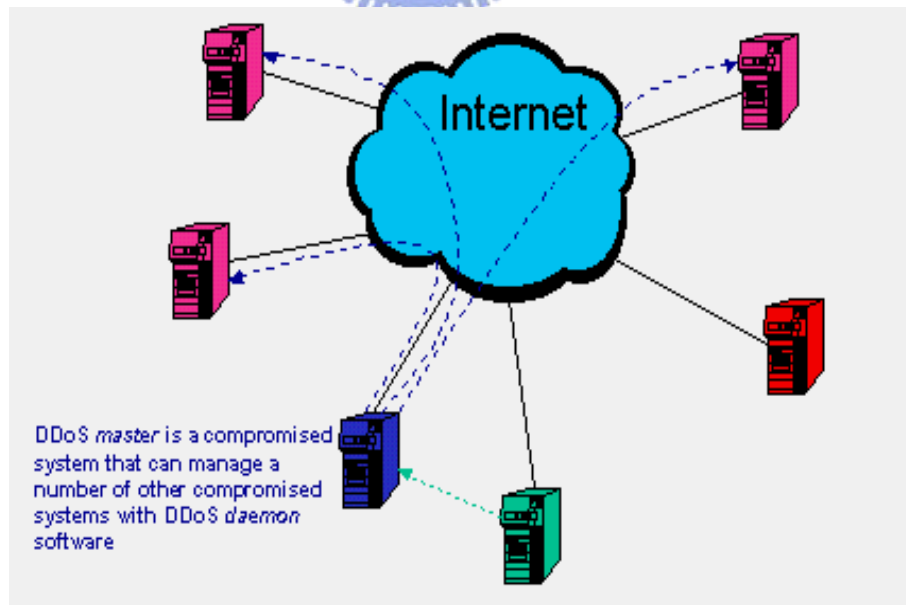


Figure 2-3 DDoS Attacking-Stage 2

( Figure Source [11] )

C. To start the attacking program from far away main control host to make the attacked hosts intrude specific websites at the same time; like Figure 2-4.

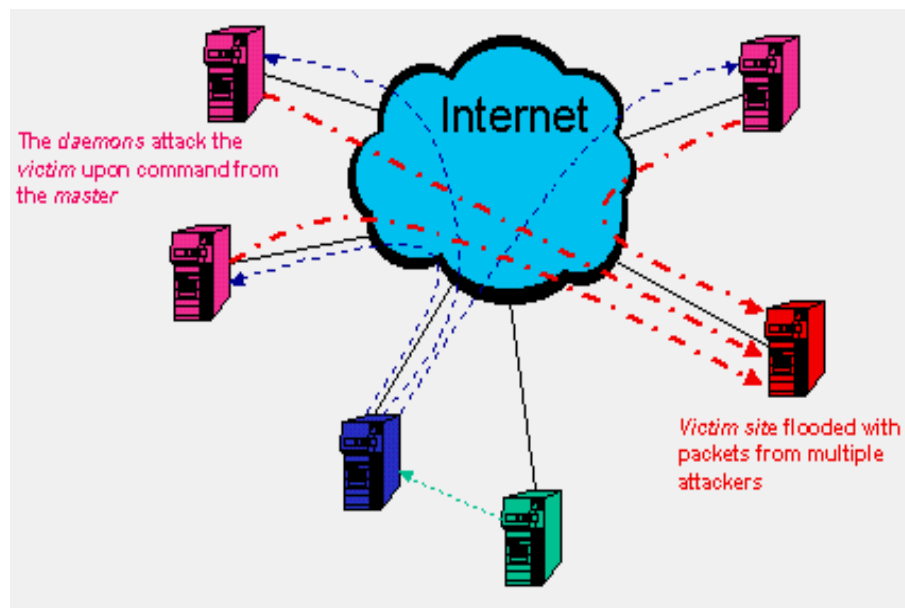


Figure 2-4 DDoS Attacking-Stage 3

( Figure source [11] )

## 2.2 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) [1] [9], can detect immediately abnormal behaviors (misuse, abuse, attack) or act against a user from its own rule of security policy. It's different from so-called Firewall; the main function of the Firewall is to execute Access Control. As long as it is not obey the rules, the packet cannot be passed. If it follows the rules or the data doesn't through the system, it cannot guarantee to provide security protection. For example, internal attacking which is behind the firewall or the accounts used by the one who is not authorized.

The IDS can be divided into two major types:

- ◆ Host-based IDS: It is mainly designed for one host. It can monitor the higher level data of Protocol Stack, like operating system or application programs. As Figure 2-5.

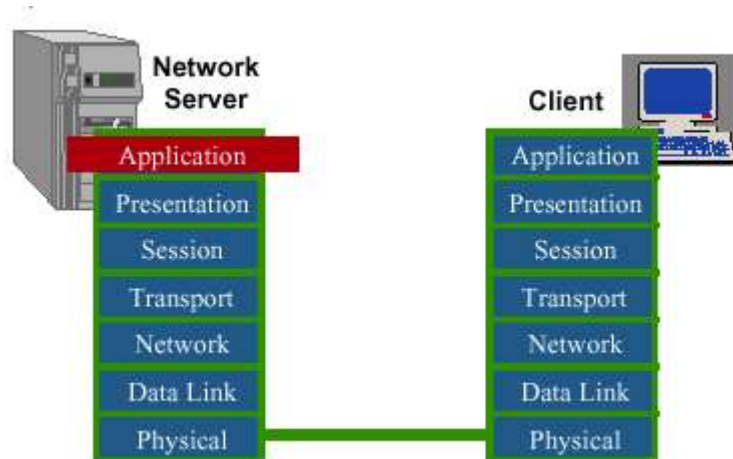


Figure 2-5 Host-based IDS

The Network-based IDS: The IDS of this thesis is NIDS. It usually supervises the data transmitted via internet. Its advantages are as below:

- A NIDS can monitor several hosts.
- IDS deployment is as figure 2-6 showed. Unlike the firewall monitors all the data in and out, it just monitors the whole internet transmissions. The firewall usually impacts the network transmitting efficiency; moreover, it becomes the bottle neck of the internet. However, IDS only monitors and doesn't impact the transmitting efficiency.

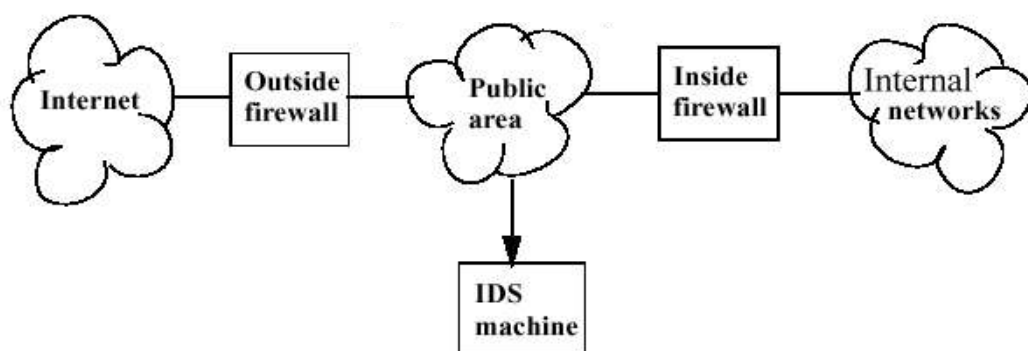


Figure 2-6 IDS deployment diagram

- Data updated (ex. renew the new rules): It is only to be done for one time, no need to update each machine one by one.
- It cannot only see the higher level data in the Protocol Stack, but also the lower packet data. As figure 2-7.

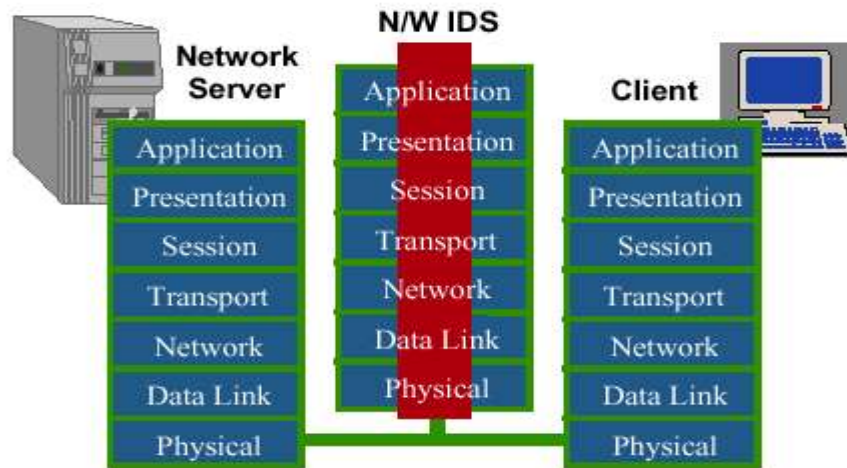


Figure 2-7 Networks-based IDS

It can detect the intrusion activities immediately; no time wasted as waiting the packets entered the machine. The function of the NIDS is not really to execute protection. The main mission is to detect the intrusion events. Usually, it detects the intrusion activities by comparing between analyzing packet flow quantity, and the noted attacking pattern.

## 2.3 IDS Snort

Snort [10] is mainly designed by Martin Roesch design. The main characteristics are as below.

- ◆ Lightweight intrusion detection system
- ◆ Instant data analyzing and logging the packets on internet
- ◆ Able to execute analysis of communication protocol, content searching and comparing



- ◆ Use libpcap to catch internet packet which the program written by C language
- ◆ Adopting Rule-based to detect intrusion; able to describe the packet to be detected with a simple language. Able to download the latest Rule database from Snort website at any time
- ◆ Adaptable to small and low flow network
- ◆ It is free software of GNU (GENERAL PUBLIC LICENSE ), and provides the source code.
- ◆ Its structure is such as figure 2-6. Making use of the Libpcap to start BPF (Berkeley Packet Filter) to catch the packet on internet and compare the string (pattern matching) with the Rule base that set up in advance. When intrusion activities are detected, it will produce log, alert or pass.

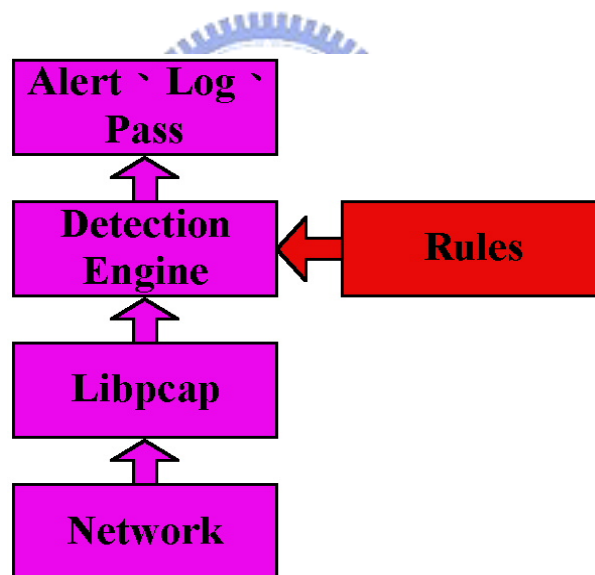


Figure 2-8 Snort Structure

### 2.3.1 Snort Rules

The rule matching of Snort is its key technique. We will introduce its applications with the rule first.

#### ※ Construction of Rule:

**Rule header + Rule options**

For example: alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any (flags: SF; msg: "SYN-FIN Scan");

|-----header-----||-----options-----|

#### ※ Rule header :

##### ◆ Action :

- Alert: Produce a warning such as writing them to syslog or flick a message Windows on the monitor of the appointed machine
- Log: To record the packets.
- Pass: Allow the packet pass without doing anything

##### ◆ Protocol :

Including three kinds of protocol: TCP, UDP, and ICMP

##### ◆ IP address:

- Use "any" for random IP
- Appointed IP address: ex.140.112.8.164.
- CIDR format: ex. 140.112.8/24.
- Able to use"!" to represent "not" what kind of the IP address, as!  
140.112.8/24, indicates not a sub-network of 140.112.8. x

◆ Port Numbers :

- . Use “any” for random Port
- . Appointed port: ex. 80,23 ...etc.
- . A scope: ex.
  - 1:2048, indicates port 1 to port 2048.
  - :1024, indicates less or equal to port 1024.
  - 512:, indicates bigger or equal port 512
- . Can use "!" to indicate "Not" what kind of the port.

◆ Direction :

- source\_ip\_port -> destination\_ip\_port : Source IP address is in the left; destination IP address is in the right.
- <> : Means it doesn't tell them from source IP address or destination IP address.



※ Rule options :

- ◆ Msg: The message that let log or alert together to be recorded.  
Language msg:”<message text>”;
- ◆ Logto: Point out the specific file which is to be save the records.  
Language logto: “<filename>;
- ◆ IP TTL: Set a condition that matches a TTL (time to live).  
Language ttl:”<number>”;
- ◆ IP ID: A setting that matches a IP Fragment ID  
Language id:”<number>”;
- ◆ Dsize: Check the size of the packet Payload.  
Language dsize: [>|<]<number>;
- ◆ Content: Searching a specific stream in the packets. If it is binary data, it will be with “|”

For example, content: "|90C8 C0FF FFFF|/bin/sh";

Language content:"<content string>";

- ◆ Offset: Comparing the streams from a specific start point.

Language offset:"<content string>";

- ◆ Depth: Only comparing the stream for some specific length of the data from packets.

Language depth:<number>;

- ◆ Nocase: Ignore the whether it is capital letter or lowercase when comparing
- Language nocase;

- ◆ Seq: The setting of the Sequence Number which matches TCP heading

Language seq:<number>;

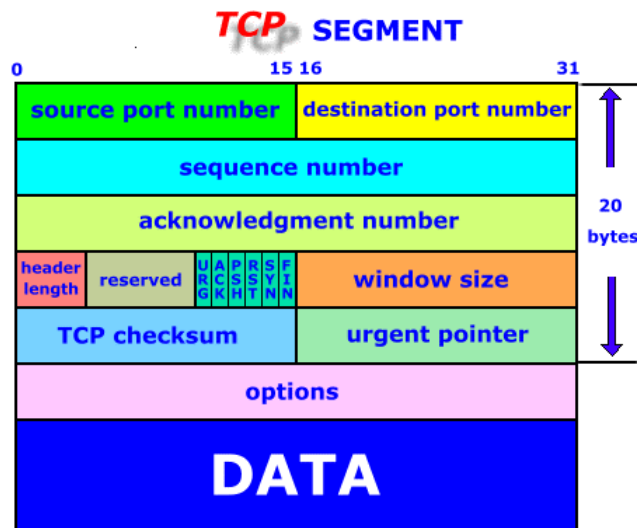


Figure 2-9 TCP Headings

( Figure Source [8] )

- ◆ **Flags:** The setting of the Flag which matches TCP heading. There are eight of Flag as below.

- F - FIN
- S - SYN
- R - RST
- P - PSH

- A - ACK
- U - URG
- 2 - Reserved bit 2
- 1 - Reserved bit 1

**Language flags:***<flag values>*;

- ◆ **Ack:** The setting of the acknowledgement number which matches TCP heading.

**Language ack:***<number>*;

- ◆ **Itype:** The setting that matches ICMP TYPE

**Language itype:***<number>*;

- ◆ **Icode:** The setting that matches ICMP VALUE.

**Language icode:***<number>*;

[Please refer to appendix 1 for ICMP TYPE and VALUE]

- ◆ **Session:** Retrieve all the data of User's TCP Session; especially in telnet, rlogin, ftp and web session. There are two kinds as below:

- Printable : Only record the data that can be read directly; like text.
- All : Transfer the data that cannot be read directly to HEX.

**Language session:***<printable/all>*;

- ◆ **Icmp\_id:** The setting of ICMP ID Number that matches ICMP ECHO packets.

**Language icmp\_id:***<number>*;

- ◆ **Icmp\_seq:** The setting of ICMP Sequence Number that matches ICMP ECHO packets.

**Language icmp\_seq:***<number>*;

- ◆ **Ioption:** Provided the function of searching some specific option

- rr - Record route
- eol - End of list
- nop - No op

- ts - Time Stamp
- sec - IP security option
- lsrr - Loose source routing
- ssrr - Strict source routing
- satid - Stream identifier

**Language ipoption :< option>;**

- ◆ **Rpc: Searching the application, procedure, and program version when using RPC.**

**Language rpc:<application number, [procedure number|\*], [program version number|\*]>**

- ◆ **Resp: Providing flexible response. There are seven kinds of resp\_modifier as below. They can be used at the same time.**

- rst\_snd - send TCP-RST packets to the sending socket
- rst\_rcv - send TCP-RST packets to the receiving socket
- rst\_all - send TCP\_RST packets in both directions
- icmp\_net - send a ICMP\_NET\_UNREACH to the sender
- icmp\_host - send a ICMP\_HOST\_UNREACH to the sender
- icmp\_port - send a ICMP\_PORT\_UNREACH to the sender
- icmp\_all - send all above ICMP packets to the sender

**Language resp:<resp\_modifier[,resp\_modifier...]>;**

### 2.3.2 Rule Tree

The Snort rule has more than 5000s about currently. It can detect various kinds of intrusion. The rule is very huge. To increase the speed of detecting, it needs to take some actions to the Rule. Snort stores Rules with the Tree pattern. First, taking Rule header as a horizontal string row, the Rule option is each Rule header under of lengthways string row, and make all Rule headers be the only one. If the repetition of the Rule header appears, then adding the string of Rule

option row directly underneath, as figure 2-10. The advantage is that the same rule headers are only being checked once and raise the speed of comparing. Although it doesn't eliminate comparing the rule Option, it doesn't matter as the repetition is not frequent.

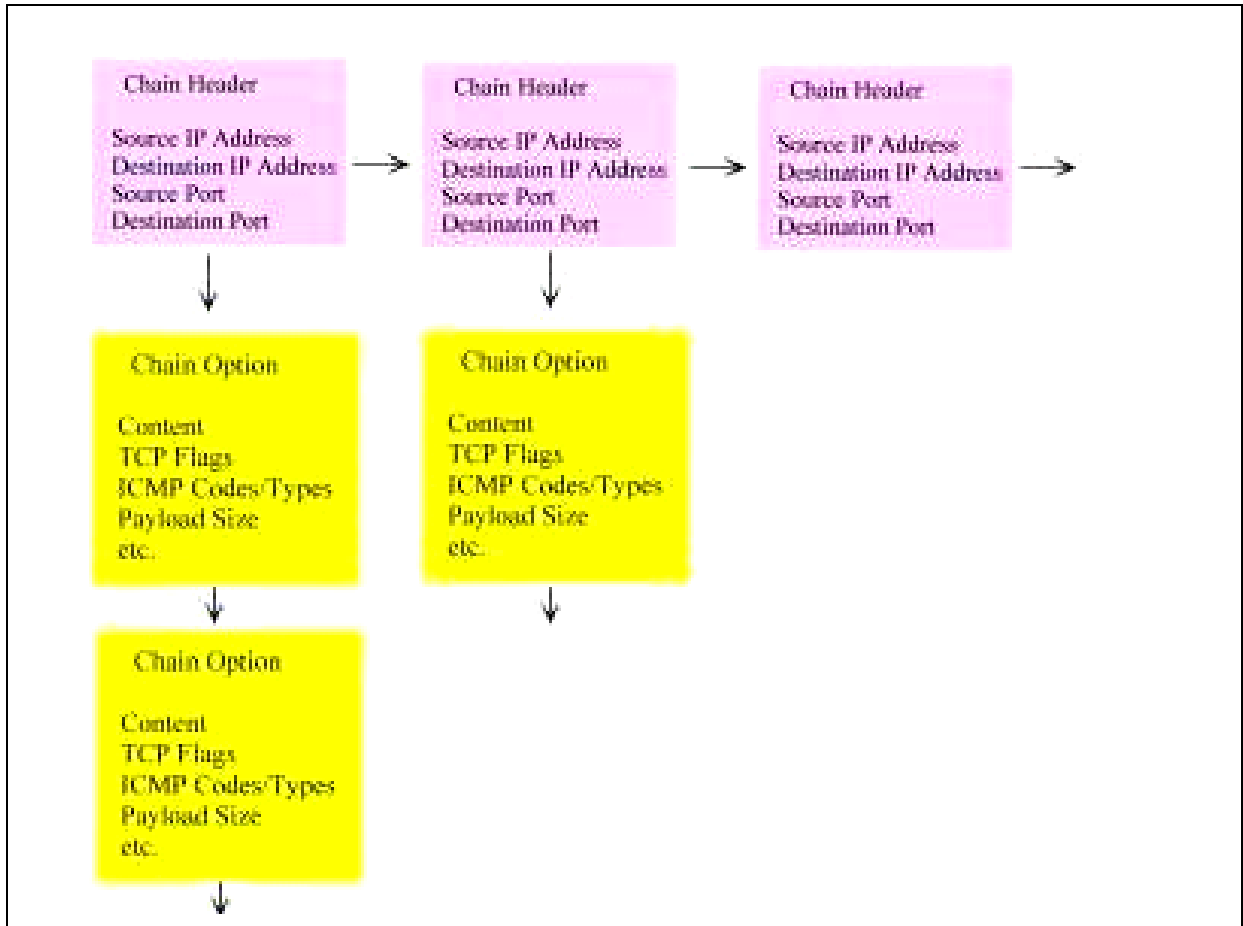


Figure 2-10 Snort Rule Tree Structure

### 2.3.3 Preprocessors

The Preprocessor makes the users be able to join their own module easily, and it execute before the packets enter the detection engine of Snort.

Language preprocessor <name>:<options>

### 2.3.4 Variables

Usually, we will edit snort.lib before using Snort. There are many variables need to be defined in advance; like your network, and IP address of

DNS.

Language <name>:<value>

### 2.3.5 Weakness


Generally speaking, the common problem of the pattern-based- IDS is the record is excessive; Snort also faces the same situation.

### 2.3.6 Snortlog analysis tool

#### ※ Snort\_stat.pl:

It is a snort log statistics program written with perl. It can produce the statistics data as follows:

- **Number of attack from same host to same destination using same method**



# of attack	from	to	With
26	140.110.21.99	140.112.10.100	PING-ICMP Time Exceeded
1	140.110.20.81	140.112.18.163	FTP-bad-login
3	140.112.10.24	140.112.18.99	IDS159-PING Microsoft Windows
...	.....	....	.....



■ **Percentage and number of attacks from a host to a destination**

<b>%</b>	<b># of attacks</b>	<b>from</b>	<b>To</b>
<b>24.46</b>	<b>32</b>	<b>140.109.20.100</b>	<b>140.112.18.164</b>
<b>12.23</b>	<b>16</b>	<b>140.109.20.80</b>	<b>140.112.8.153</b>
<b>5.35</b>	<b>7</b>	<b>140.112.12.34</b>	<b>140.112.8.98</b>
<b>...</b>	<b>...</b>	<b>...</b>	<b>...</b>

■ **Percentage and number of attacks from one host to any with same method**



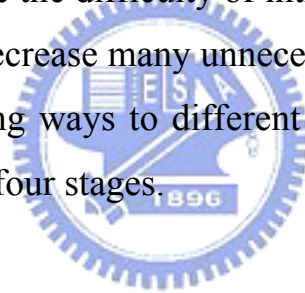
<b>%</b>	<b># of attacks</b>	<b>from</b>	<b>Type</b>
<b>17.95</b>	<b>14</b>	<b>140.109.30.10</b>	<b>ICMP Destination Unreachable</b>
<b>15.38</b>	<b>15</b>	<b>140.109.30.80</b>	<b>ICMP Destination Unreachable</b>
<b>12.89</b>	<b>11</b>	<b>140.112.12.34</b>	<b>PING-ICMP Time Exceeded</b>
<b>...</b>	<b>...</b>	<b>...</b>	<b>...</b>

# CHAPTER 3

## IP STATUS DATABASE

### 3.1 Intrusion Behavior Analysis

An intrusion event occurred usually isn't by chance. The hacker wants to intrude a system is just like a commando permeate into a castle. It must have a detailed and complete plan. The complication of the plan depends on the safety level of the system. First, it collect information and overview its target, because blindly trial reveals the sign of intrusion very easily and the one intruded alerts to guard and increase the difficulty of intrusion. Therefore, once we have a specific target, we can decrease many unnecessary trial and error. For example, there are different attacking ways to different systems, and servers. Below, we will divide intrusions into four stages.



#### ✂ **Stage One: Information Collecting**

The information collection let the attackers get more useful information of the attacked one. For example, the safety measures (whether if it sets up firewall or not, IDS...etc.), the allocation of intranet IP, stir to answer the phone number (some of the string network can be hided from the checking of firewall), and branch (possibly the authorized IP which passed from the IP-Based access control ...etc. Making use of some current tooling and technology, the attackers can get some information automatically. For example:

- ◆ Finger, whois: The command to obtain the user information.
- ◆ Traceroute: The path tracking program which acknowledge the routers passed by, or the possible existent firewall. However, currently there are many units have already closed traceroute.

- ◆ Teleport Pro: It can duplicate the contents of the target website automatically, then find out useful information from them. Some websites establish a program that can create a great deal of faulty data to prevent being duplicated.

## ❖ Stage two: Network Scanning

- ◆ An entrance of a normal house is its front door, but for the sneaks, it can be windows, back door, and chimney...etc. Network Scanning is to find out the host of the attack target and the services it provides. It makes use of the channels and possible safety leak. The so-called portscan( scanning conjunction) is exactly the hacker often use for dictation beforehand. By using portscan, the hackers can find out a network operation in active and each port that can provide services of all machines. There are two types of portscan:
  - ◆ Scanning the entire network: It usually scan the IP address in the order from small (big) to the big (small) IP one after another. It mainly is to know to how many active machines are.
  - ◆ Scanning all the connectors of each machine: Scanning from small (big) connectors to big (small) ones one by one. It mainly is to know the services that provided by the hosts.

## ❖ Stage Three: The weakness attack

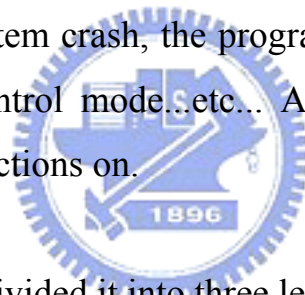
After understanding the services and operation system of the target host, the hackers can launch the intrusion attack to the related weakness. For example, a server opens port 80 or 8080, so that it maybe a web server, then the intruder can find out the web program and version used, and taking use of related web attacking program to start intrusion.

## ❖ Stage four: Obtain the Right of Usage

The final purpose that attacker makes series of intrusion activities is to obtain the right of usage (general user), control root or install particular program, such as backdoor program, DDoS master or daemon ...etc. With these rights means that the hacker can control the host completely, it can set up false account and obtain confidential data in the host...etc.

## 3.2 Dividing the Rules into Urgency Levels

In the Snort intrusion detection rules, in fact it is separated by different safety urgency. For example, ftp-bad-login is to record ftp on-line register errors. Such event is not necessarily a very urgent intrusion event. Moreover, it often includes typo from normal users. However, some events like the overflows, usually may cause the system crash, the program breaks off abnormally or even jumped to the system control mode...etc... Above emergency events possibly need immediately taking actions on.



For Snort rule, we divided it into three levels:

- ◆ High: The events those needs to be handled immediately; like it may obtain the root legal power or cause the system crash.
- ◆ Medium: Although it doesn't immediately cause damages, it may follow with DDoS attack.
- ◆ Low: "Possible" attacking events, like MISC-PCAnywhere Attempted Administrator Login.

As different administrators may have different definitions for each emergency degree of various rules, so the rule emergency level can be defined by users. We have already set up the rule grade as appendix two.

### 3.3 Build IP Status Database

According to the harmfulness degree of the intrusion records, we can give IP a different status according to the behavior of different stage. We divide it into three kinds of grades:

- ◆ Hostile: IP possibly is attacking.
- ◆ Threaten: IP may be potential offensive
- ◆ Suspicious: IP with suspicious behavior.

For example, the activity of finger, scan, and the ping ...etc. is generally the behavior that belongs to intrusion preliminary, the IP with records like this is included in "Suspicious" grade. When this IP is the records those belong to Medium grade, then it is upgrade to "Threatening" grade. At the end, if they are the events those belong to High, it will be raised as the highest grade "Hostile". We illustrate this with status figure 3-1.

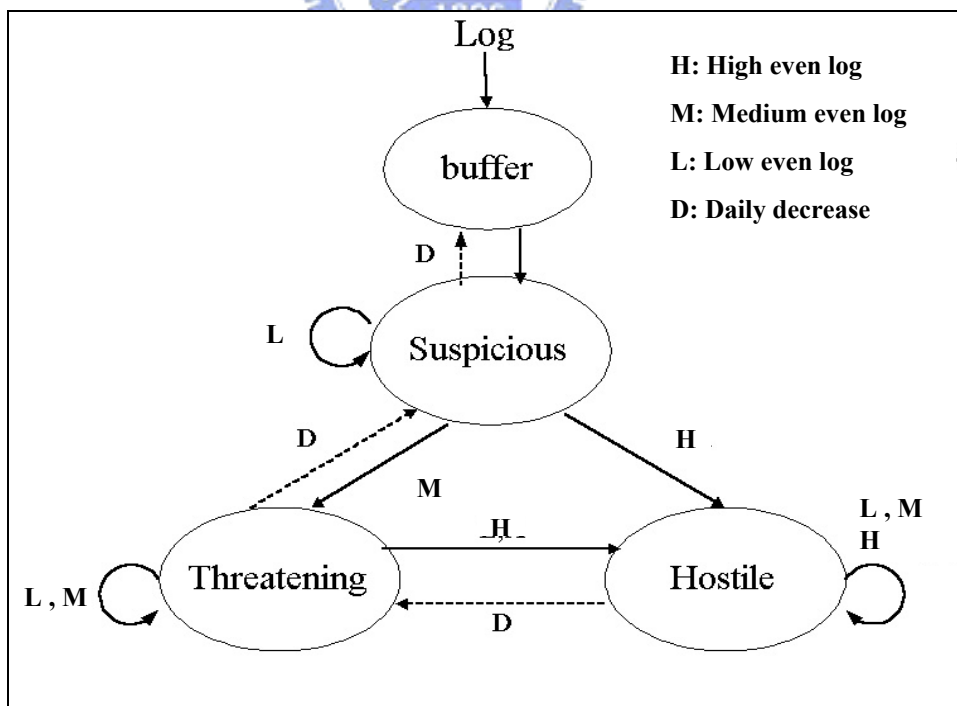


Figure 3-1 BAD IP finite state

- ◆ When "Low" of a new IP records number is bigger than a certain minimum value, then it will get into "Buffer" status of the database. At the moment, it still doesn't belong to any grade. However, if the number is bigger than the minimum value of "Suspicious", then it directly gets into "Suspicious" status.
- ◆ When IP is at "Suspicious" status, if there is "Low" events happened, then it will stay in the original status. Once "Medium" events occurred, it will be transferred to "Threatening" status. If there is "High" event, then it directly turns into "Hostile" status.
- ◆ When IP is at "Threatening" status, if there is "Low" or "Medium" happened then it will stay the original status. Once "High" event occurs, it turns into "Hostile" status.
- ◆ When IP is at "Hostile" status, if there is any record occurs, then it stays original status.
- ◆ Each IP may still stay in the condition of original status for different events, but its scores will have different scores increment with the amount of events occurred.
- ◆ Each IP will gradually decrease its scores everyday. Different status may have different decreasing value till to zero, because the attacking to a host usually is in a short time like one month or even one week, two or three days. The attack will not take actions in a long time interval.
- ◆ IP and status database can choose not using day as a unit, for example, every half day, or every hour to be processed once. As long as you adjust the parameter of the transformation ratio between the times and the scores, and the value of gradually decreased per day.

The high or low scores of each IP represent different possible damage degree. The parameters that user can define by itself are as below:

- ◆ Deposit the least score (the minimum value of Buffer State) into the BAD IP database: When the IP score is lower than this value, it doesn't be deposited into this database.
- ◆ The minimum score of Hostile: The score that higher than this value means the IP is hostile.
- ◆ The minimum score of Threatening: The score that higher than this value means the IP is threatening.
- ◆ The minimum score of Suspicious: The score that higher than this value means the IP is suspicious.
- ◆ The conversion ratio between the times and scores
- ◆ The scores gradually decreasing per day

### 3.4 Records Analysis

Due to different levels of intrusion kinds and IP source address, we constructed a 3 X 3 two-weight matrix form to analysis the Snort record logs, as table 3-1. Take blank (5) as an example, there are two kinds of modes-And, and Or in total. And indicates that the rule grade is Alert (contain) above and IP is threatening grade above. Therefore, it is the range of blank (1-2), and blank (4-5). Or indicates that the rule grade is Alert (contain) above or the suspicious score is above medium level; so it is the range of the blank (1-8).

Table 3-1 Records Analysis Table

Rule Type Point	High	Medium	Low
Hostile	And (1) Or	And (2) Or	And (3) Or
Threatening	And (4) Or	And (5) Or	And (6) Or
Suspicious	And (7) Or	And (8) Or	And (9) Or

"Any" in the table 3-1 indicates it includes all whether if the IP appears in the database or not. In other words, it has no restriction at all. The Or in the rightist line and the lowest column have the same times. It equals to all the records, because the minimum value of each grade is "Notification" and "Any", the total is only 25 combinations.

Indicate the times of each combination with the form of array:

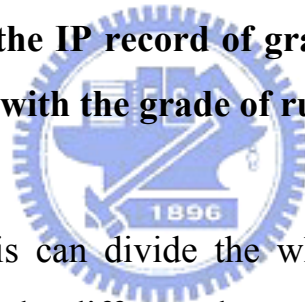
- ◆ A (n, m), O :( n, m): It is the times of And or Or respectively.
- ◆ n: This indicates rule grade increasing from left to right. (High=1, Low=3)
- ◆ m: This indicates a suspicious scores increasing from top to bottom. (Hostile=1,Suspicious=3)
- ◆ The whole times table is such as table 3-2.



Table 3-2 Record Analysis Quantity Statistics Table

<b>A(1,1)</b>	<b>A(2,1)</b>	<b>A(3,1)</b>
<b>O(1,1)</b>	<b>O(2,1)</b>	<b>O(3,1)</b>
<b>A(1,2)</b>	<b>A(2,2)</b>	<b>A(3,2)</b>
<b>O(1,2)</b>	<b>O(2,2)</b>	<b>O(3,2)</b>
<b>A(1,3)</b>	<b>A(2,3)</b>	<b>A(3,3)</b>
<b>O(1,3)</b>	<b>O(2,3)</b>	<b>O(3,3)</b>

- We can get  $A(i,j) \geq A(k,l)$  for  $i \geq k$  and  $j \geq l$   
 $O(i,j) \geq O(k,l)$  for  $i \geq k$  and  $j \geq l$
- **A(n,3): It is the records grade of High · Medium or Low; it is not related with IP.**
- **A(3, m):It is the IP record of grade for each level of damage; it is not related with the grade of rule.**



Such record analysis can divide the whole records into many different grades levels, and provide the different demands of information for users. For example, the A(1,1) is the most important record, it only includes the records which the IP is "Emergency" and the hostile; the O(1,1) is the record which indicates to check the records which matches "Emergency" or hostile IP address. When users want to see more data, they can choose A(1,2), A(2,1) or A(2,2) ...etc. for other parts of the data.

Due to that the blanks excluded A (1,1) at least include two kinds or above rule grade and different damage level of IP address, we mark the data with different colors for each rule grade and IP to make the differentiation; like the records data as below.

---

[\*\*] IDS127 - TELNET - Login Incorrect [\*\*]

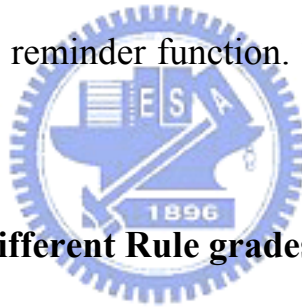
05/31-23:24:09.581436 140.112.8.79:23 -> 140.112.240.40:2018

TCP TTL:255 TOS:0x0 ID:42821 IpLen:20 DgmLen:59 DF

\*\*\*AP\*\*\* Seq: 0x196D55F2 Ack: 0x4BC27875 Win: 0x2238 TcpLen: 20

---

Indicate rule-"IDS127- TELNET- Login Incorrect" belongs to Low grade, and the IP-140.112.8.79 belongs to Threatening grade. This analysis surveillance program can be used for looking into the history data. It can also show the setting conditions based on real time records on the console while in the mode of command executing and showing the real time analysis. It also provides the beep beep sounds in the meantime while a record matching the condition to strengthen the reminder function. The ways of differentiation are as below:



◆ **The colors for different Rule grades**

- High-red.**
- Medium-blue.**
- Low-green.**

◆ **The colors for different damage degree of IP address**

- Hostile-red.**
- Threatening-blue.**
- Suspicious-green.**

Based on the two different measurement index numbers, the data has different importance levels. Moreover, it is able to decrease the confusion caused

by too much records. The structure of the whole record analysis system is built up with snort. It makes use of rules and IP ratings as a basic database to analyze records, like the blue part of the structure figure 4-2. It is included "Leveled Rules", "BAD IP" and "Analyzer".

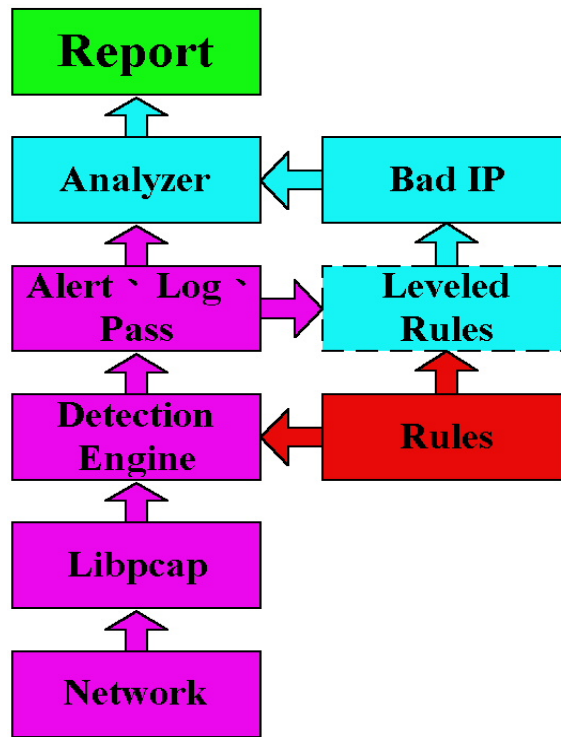


Figure 3-2 Configuration of Records Analysis System

# CHAPTER 4

## SNORT LOG ANALYSIS

### 4.1 Tests Environment

- ◆ Snort: Version 2.6.1 with 5850 rules currently
- ◆ Host: PCIII-550 RAM: 1024 MB
- ◆ Operation system: Linux Kernel 2.6.12
- ◆ Measurement location: No. 6, Lane 37, Jieyun Rd., Sanchong City, Taipei County 241, Taiwan ( R.O.C.) ( 寶石典藏家 )
  - There are 199 machines which are registers in this area.
  - The whole backbone of the area is a CISCO 7513 Switches, providing surveillance of all the flow from in and out of port mirror and the port that connect to the Snort machine.
- ◆ Measurement period: About 50 days ( 2007/9/12 ~ 2007/10/31 )
- ◆ Network Structure:

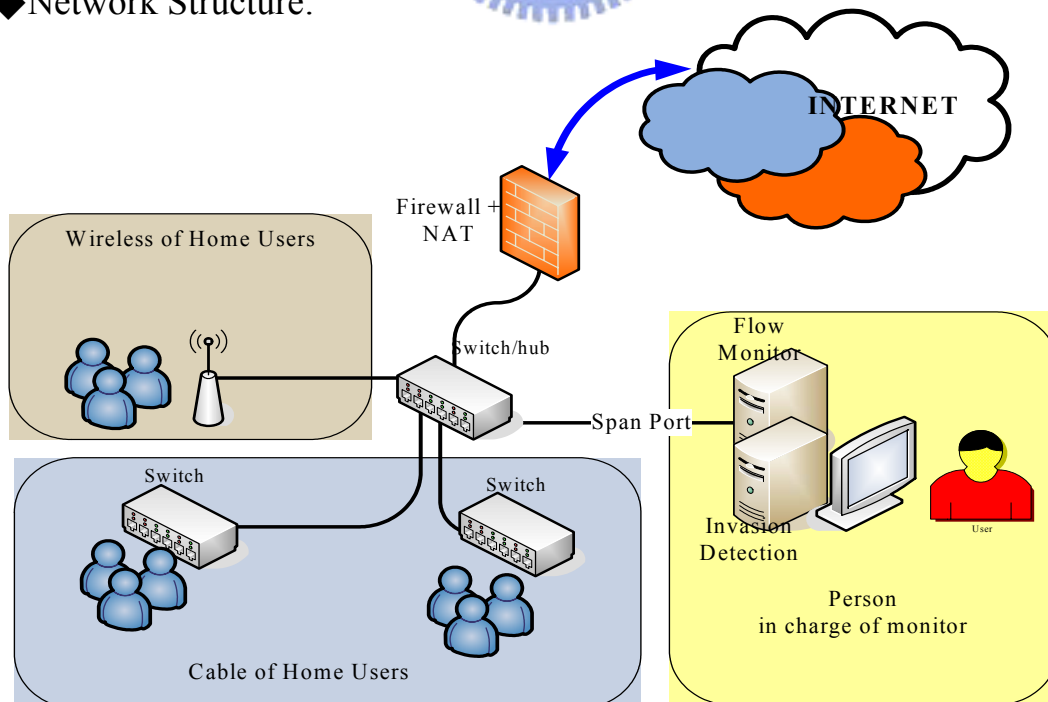


Figure 4-1 Snort Record Analysis System

- For the whole database, it provides:  
Setting or Rule Grade: Set or modify the emergency level of the rule.

### Snort Log Analysis System

Select a type to set security level

<a href="#">Attack-response</a>	17	<a href="#">Icmp</a>	22	<a href="#">Misc</a>	71	<a href="#">Content-replace</a>	12	<a href="#">Nntp</a>	14
<a href="#">Dos</a>	37	<a href="#">Imap</a>	70	<a href="#">Chat</a>	36	<a href="#">Finger</a>	14	<a href="#">Porn</a>	28
<a href="#">Ftp</a>	82	<a href="#">Icmp-info</a>	93	<a href="#">Ddos</a>	32	<a href="#">Info</a>	11	<a href="#">Multimedia</a>	13
<a href="#">Backdoor</a>	723	<a href="#">Bad-traffic</a>	14	<a href="#">Dns</a>	25	<a href="#">Mysql</a>	14	<a href="#">P2P</a>	28
<a href="#">POP3</a>	36	<a href="#">POP2</a>	4	<a href="#">Other-ids</a>	3	<a href="#">Oracle</a>	322	<a href="#">Scan</a>	21
<a href="#">X11</a>	2	<a href="#">Web-php</a>	145	<a href="#">Web-misc</a>	396	<a href="#">Web-iis</a>	143	<a href="#">Web-frontpage</a>	38
<a href="#">Web-coldfusion</a>	43	<a href="#">Web-client</a>	1329	<a href="#">Web-cgi</a>	369	<a href="#">VoIP</a>	62	<a href="#">Virus</a>	7
<a href="#">Tftp</a>	15	<a href="#">Telnet</a>	22	<a href="#">Sql</a>	86	<a href="#">Spware-put</a>	791	<a href="#">Specific-thread</a>	132
<a href="#">SNMP</a>	18	<a href="#">SMTP</a>	95	<a href="#">Rservice</a>	14	<a href="#">Shellcode</a>	32	<a href="#">RPC</a>	156
<a href="#">Exploit</a>	213								
Total Rule:5850									

#### Type Attack-response Rule

ATTACK-RESPONSES directory listing---High  
 ATTACK-RESPONSES command completed---High  
 ATTACK-RESPONSES command error---High  
 ATTACK-RESPONSES file copied ok---High  
 ATTACK-RESPONSES Invalid URL---High  
 ATTACK-RESPONSES index of /cgi-bin/ response---High  
 ATTACK-RESPONSES 403 Forbidden---High  
 ATTACK-RESPONSES id check returned root---High  
 ATTACK-RESPONSES id check returned userid---High  
 ATTACK-RESPONSES oracle one hour install---High

High
  Medium
  Low

Figure 4-2 Picture of Rule Grade Setting

- Rule table: Show the rule of the database by its type or grade.

### Snort Log Analysis System

Select a type to set security level

<a href="#">Attack-response</a>	17	<a href="#">Icmp</a>	22	<a href="#">Misc</a>	71	<a href="#">Content-replace</a>	12	<a href="#">Nntp</a>	14
<a href="#">Dos</a>	37	<a href="#">Imap</a>	70	<a href="#">Chat</a>	36	<a href="#">Finger</a>	14	<a href="#">Porn</a>	28
<a href="#">Ftp</a>	82	<a href="#">Icmp-info</a>	93	<a href="#">Ddos</a>	32	<a href="#">Info</a>	11	<a href="#">Multimedia</a>	13
<a href="#">Backdoor</a>	723	<a href="#">Bad-traffic</a>	14	<a href="#">Dns</a>	25	<a href="#">Mysql</a>	14	<a href="#">P2P</a>	28
<a href="#">POP3</a>	36	<a href="#">POP2</a>	4	<a href="#">Other-ids</a>	3	<a href="#">Oracle</a>	322	<a href="#">Scan</a>	21
<a href="#">X11</a>	2	<a href="#">Web-php</a>	145	<a href="#">Web-misc</a>	396	<a href="#">Web-iis</a>	143	<a href="#">Web-frontpage</a>	38
<a href="#">Web-coldfusion</a>	43	<a href="#">Web-client</a>	1329	<a href="#">Web-cgi</a>	369	<a href="#">VoIP</a>	62	<a href="#">Virus</a>	7
<a href="#">Tftp</a>	15	<a href="#">Telnet</a>	22	<a href="#">Sql</a>	86	<a href="#">Spware-put</a>	791	<a href="#">Specific-thread</a>	132
<a href="#">SNMP</a>	18	<a href="#">SMTP</a>	95	<a href="#">Rservice</a>	14	<a href="#">Shellcode</a>	32	<a href="#">RPC</a>	156
<a href="#">Exploit</a>	213								
Total Rule:5850									

Rule	Security Level
<b>Web-client</b>	
WEB-CLIENT Outlook EML access	Medium
WEB-CLIENT Microsoft emf metafile access	Medium
WEB-CLIENT Microsoft wmf metafile access	Medium
WEB-CLIENT XMLHttpRequest attempt	Medium
WEB-CLIENT readme.eml download attempt	Medium
WEB-CLIENT readme.eml autoload attempt	Medium
WEB-CLIENT Javascript document domain attempt	Medium
WEB-CLIENT Javascript URL host spoofing attempt	Medium
WEB-CLIENT RealPlayer arbitrary javascript command attempt	Medium

Figure 4-3 Picture that rule showed by its type

### Rule list sorted by level

Rule Level		
TYPE	Rule	LEVEL
ATTACK-RESPONSES	ATTACK-RESPONSES directory listing	High
ATTACK-RESPONSES	ATTACK-RESPONSES command completed	High
ATTACK-RESPONSES	ATTACK-RESPONSES command error	High
ATTACK-RESPONSES	ATTACK-RESPONSES file copied ok	High
ATTACK-RESPONSES	ATTACK-RESPONSES Invalid URL	High
ATTACK-RESPONSES	ATTACK-RESPONSES index of /cgi-bin/ response	High
ATTACK-RESPONSES	ATTACK-RESPONSES 403 Forbidden	High
ATTACK-RESPONSES	ATTACK-RESPONSES id check returned root	High
ATTACK-RESPONSES	ATTACK-RESPONSES id check returned userid	High
ATTACK-RESPONSES	ATTACK-RESPONSES oracle one hour install	High
ATTACK-RESPONSES	ATTACK-RESPONSES successful kadmin buffer overflow attempt	High
ATTACK-RESPONSES	ATTACK-RESPONSES successful kadmin buffer overflow attempt	High
ATTACK-RESPONSES	ATTACK-RESPONSES successful gobbles ssh exploit GOBBLE	High
ATTACK-RESPONSES	ATTACK-RESPONSES successful gobbles ssh exploit uname	High
WEB-CLIENT	WEB-CLIENT Content-Disposition CLSID command attempt	Medium
WEB-CLIENT	WEB-CLIENT bitmap BitmapOffset integer overflow attempt	Medium
WEB-CLIENT	WEB-CLIENT libpng tRNS overflow attempt	Medium
WEB-CLIENT	WEB-CLIENT JPEG parser heap overflow attempt	Medium
WEB-CLIENT	WEB-CLIENT JPEG transfer	Medium
WEB-CLIENT	WEB-CLIENT JPEG parser multipacket heap overflow	Medium
WEB-CLIENT	WEB-CLIENT Microsoft ANI file parsing overflow	Medium
WEB-CLIENT	WEB-CLIENT winamp .cda file name overflow attempt	Medium
WEB-CLIENT	WEB-CLIENT PNG large image width download attempt	Medium

Figure 4-4 Picture that rule showed by its level

- Placing of source IP address: Ranking each source IP from the detected records, and providing related records data of each IP.

The screenshot shows the Snort Log Analysis System web interface in a Netscape browser. The page title is "Snort Log Analysis System" and the sub-header is "Sorted Source IP". Below the header is a table with two columns: "IP" and "Rate". The table lists 15 IP addresses sorted by their rate in descending order.

IP	Rate
<a href="#">203.72.43.237</a>	64916
<a href="#">203.72.43.238</a>	48833
<a href="#">210.70.186.102</a>	29928
<a href="#">202.133.224.136</a>	5700
<a href="#">211.72.159.68</a>	5679
<a href="#">211.78.1.3</a>	5621
<a href="#">211.21.17.107</a>	5522
<a href="#">210.58.94.141</a>	5318
<a href="#">140.113.1.245</a>	5314
<a href="#">140.137.200.20</a>	3638
<a href="#">203.207.0.200</a>	2845
<a href="#">140.112.60.105</a>	2720
<a href="#">210.58.98.4</a>	1790
<a href="#">210.68.37.90</a>	1067

Figure 4-5 Picture of source IP address placing

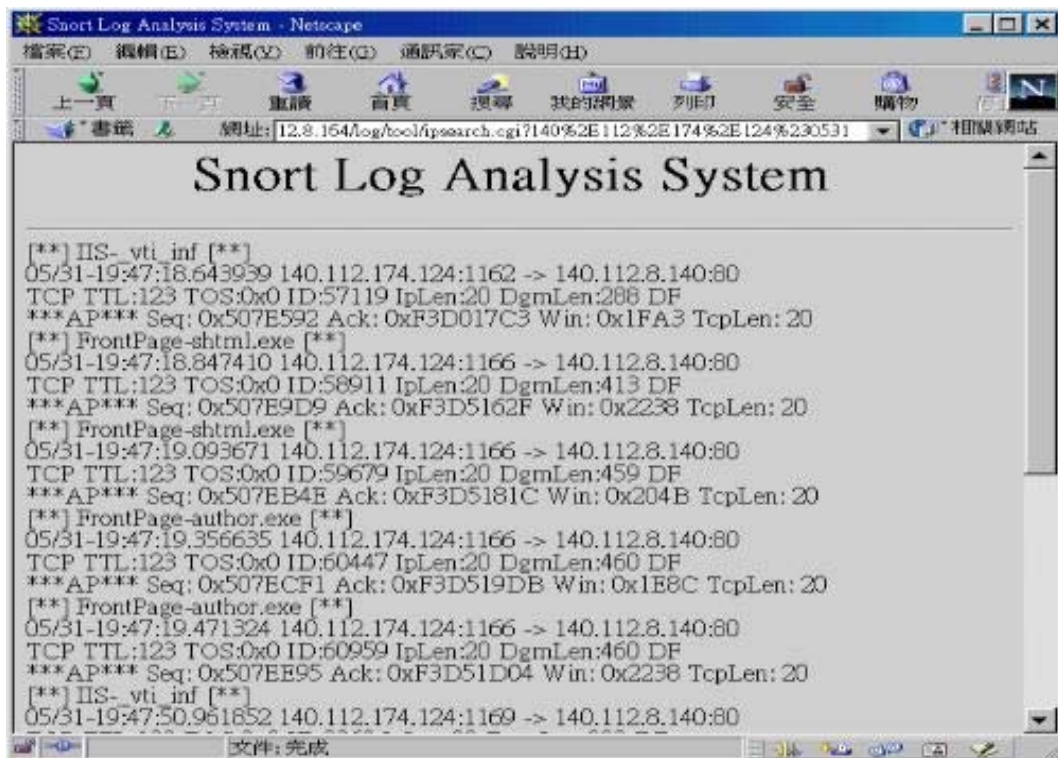


Figure 4-6 Picture of related IP records

□ Placing of the Destination IP address: Ranking each destination IP numbers from detected records, and providing related records data of each IP. Figure is the same as figure 4-5, 4-6

□ Records Analysis: Providing records analysis table. Providing records data of different demand level based on the different conditions.

## Snort Log Analysis System

Point	High	Medium	Low
<b>Bad IP</b>			
<b>Hostile</b>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>
<b>Threat</b>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>
<b>Suspicious</b>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>	<a href="#">And</a> <a href="#">Or</a>

Figure 4-7 Records Analysis Table

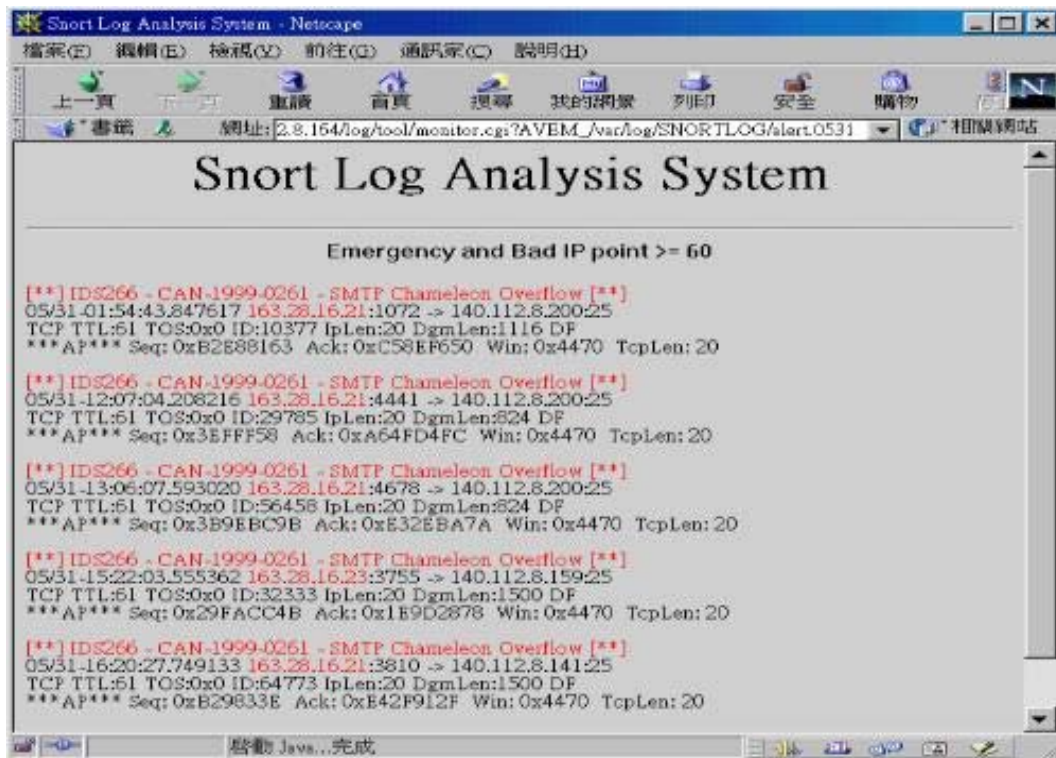


Figure 4-8 Records Analysis Example

The records those are Emergency and Threatening IP above.

◆ The function of the command line:

- Real Time Surveillance: According to the level to be servile; it shows the data which matches in real time. Meantime, it has beep beep sounds for alert.



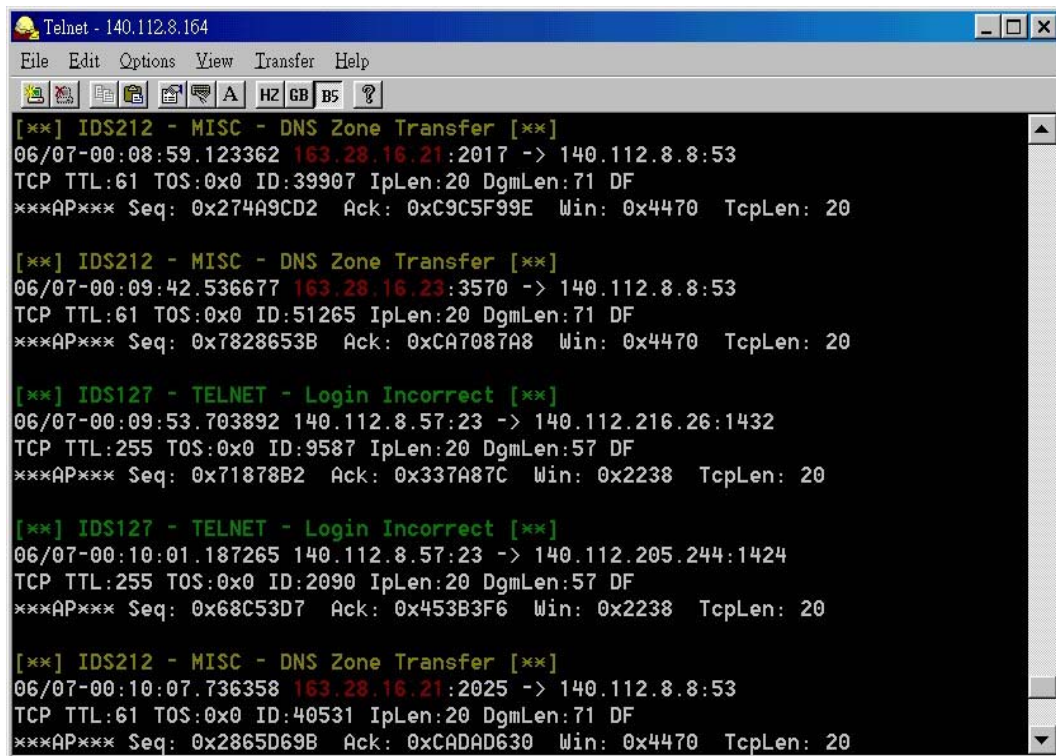


Figure 4-9 Real Time Surveillance

Define the trusted host: In the file “Trust.list”, user can define the IP which is trusted. Therefore, the records will not be showed. The format is as below.

```

=====
163.28.16.21
163.28.16.23
.....
=====

```

Searching history data of specific IP: Once we find a suspicious IP, we may want to know its process of intrusion or we would like to check if there is any attacking event of a specific IP; then we can use the command “ipserach2.pl” to search it.

Language: ipsearch2.pl *the ip to be searched* Beginning Date Finished Date

Example: ipserach2.pl 140.112.8.164 0501 0530

## 4.3 Tests Result

### ※ The Size of the Record File

The network environment of Snort is as described in previous section. Average flow is about ten or more Mb/s, the most one mostly is not over 30 Mb/s. However, the record file of everyday is more than ten Mbytes above, as table 4-1. The most one even reach 37 Mbytes. It is really a very huge data quantity.

Table 4-1 Size of Snorts Records File

Date ( Year 2007 )	File Size ( Bytes )	Records numbers ( Items )	Date ( Year 2007 )	File Size ( Bytes )	Records numbers ( Items )
09/12	23888739	183661	10/07	27395765	138070
09/13	7866625	69659	10/08	17987631	108827
09/14	18916800	123334	10/09	37423988	205125
09/15	18721438	126674	10/10	16106656	100655
09/16	24039934	158980	10/11	23542112	154465
09/17	17838936	119126	10/12	33004458	227183
09/18	18323942	173947	10/13	16083128	117531
09/19	20873982	136135	10/14	23045466	147888
09/20	14416870	98067	10/15	17066262	119095
09/21	13154609	80062	10/16	28497143	170189
09/22	14322174	90939	10/17	8704657	61528
09/23	17466491	101421	10/18	16112855	103875
09/24	16988509	107817	10/19	33854697	205853
09/25	10745145	72626	10/20	10352759	60093
09/26	11640110	81083	10/21	13495167	99732
09/27	14109060	92880	10/22	12003692	83907
09/28	11080505	75081	10/23	12701647	81080
09/29	13880252	93800	10/24	12297839	89001
09/30	14728887	79976	10/25	13135395	80612
10/01	10849316	74034	10/26	18024435	118231
10/02	9742692	65900	10/27	10483621	78223
10/03	14391299	90713	10/28	11823939	83877
10/04	12706450	86909	10/29	13782562	90121
10/05	11580967	76902	10/30	15102451	90274
10/06	26720904	201910	10/31	15004818	90071

## ※ Setting of the Related Parameter:

The minimum scores to deposit in BAD IP database: 10.

Hostile minimum scores: 60.

Threatening minimum scores: 40.

Suspicious minimum scores: 20.

The transfer ratio between numbers and scores:

Portscan log: 10

Notification log: 10

The Score gradually decreasing everyday:

Hostile: 1.0

Threatening: 1.0

Suspicious: 1.0

## ※ Records Analysis Quantity Statistics Result

In the figure 4-10, 11 and 12, we take the situation after 30, 40 and 50 days to see the number of record analysis. Take the grade above record of " Medium " level above for example, we can see from table 4-2 second row, there is about only more than 90 records. It is 0.26 % ~ 0.29 % of all the records. There are only around 80 to 100 more records of " Medium " and " Thraet " above. It is 0.29 % ~ 0.30 % of all the records. Thus, we can find out an important record from the huge data and reduce the readability difficulty of record file.

## Snort Log Analysis System

---

1011

	High	Medium	Low
<b>Hostile</b>	1 30335	86 30398	98 30954
<b>Threat</b>	1 30419	88 30598	98 30974
<b>Suspicious</b>	1 30682	91 30825	152 31347

Figure 4-10 Record Analysis Quantity Statistics Table after 30 days

## Snort Log Analysis System

---

1021

	High	Medium	Low
<b>Hostile</b>	8 32745	94 32832	164 33792
<b>Threat</b>	8 32995	96 33082	169 35042
<b>Suspicious</b>	8 33915	98 34082	170 36042

Figure 4-11 Record Analysis Quantity Statistics Table after 40 days

# Snort Log Analysis System

1031

	High	Medium	Low
<b>Hostile</b>	4 30121	93 31135	152 33806
<b>Threat</b>	4 31015	95 32154	163 34158
<b>Suspicious</b>	4 31106	98 35581	168 38154

Figure 4-12 Record Analysis Quantity Statistics Table after 50 days

Table 4-2 Comparison with using record analysis system and original records

<b>Day</b> <b>Level</b>	<b>30 days</b>	<b>40 days</b>	<b>50 days</b>
<b>Records of “ Medium ” level above</b>	( 91 / 30825 ) 0.26 %	( 98 / 34082 ) 0.29 %	( 98 / 35581 ) 0.28 %
<b>Records of “ Medium ” level and “ Threat ” above</b>	( 88 / 30598 ) 0.29 %	( 96 / 33082 ) 0.29 %	( 95 / 32154 ) 0.30 %

# CHAPTER 5

## CONCLUSION

As internet becomes popular, attacking via internet does not only have no problem of time and space but also causes the attacked loss a lot. DDoS attacking threaten E-Commerce greatly, even both Yahoo, and CNN can't resist. Among the current solutions, it is also the trend to protect the individual network to stop a DDoS network construction. Installing correction program, and build firewall are already the most basic action. Network intrusion system is able to supervise many machines. It is emphasized as its advantage of no impact to the internet transmission. However, for the most used one-rule-based NIDS, its common disadvantage is record excessive problem. It usually causes MIS members confusions of reading the records.

This thesis analyzes the attacking behaviors based on rule levels of "High", "Medium", and "Low". In the meantime, the suspicious IP will be divided into three status of "Hostile", "Threatening", and "Suspicious". Building an IP status database to analyze records, and dividing the records based on the importance of rule and IP levels; those provides MIS members supervise internet intrusion activities real time and effectively.

# REFERENCE

- [1] Jason Barlow, Woody Thrower, “The ‘TFN2K’ distributed denial of service attack tool”, 2000  
[http://packetstorm.securify.com/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt)
- [2] Wen-Chu Shen, “網路安全監控與攻擊行為之分析與實作”, 2001
- [3] C.P.S.T. Ltd., “TCP SYN Flooding Attack and the FireWall-1 SYNDefender”, Oct. 1996  
<http://www.checkpoint.com/products/firewall-1/syndefender.html>
- [4] David Dittrich, “The ‘trin00’ distributed denial of service attack tool”, 1999  
<http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt>
- [5] David Dittrich, “The ‘Tribe Flood Network’ distributed denial of service attack tool”, 1999  
<http://staff.washington.edu/dittrich/misc/tfn.analysis.txt>
- [6] David Dittrich, “The ‘stacheldraht’ distributed denial of service attack tool”, 1999  
<http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>
- [7] Thomer M. Gil, “MULTOPS:a data strycture for denial-of-service attack detection”, August, 2000  
[http://pdos.lcs.mit.edu/thomer/mit/multops\\_usenix2001.pdf](http://pdos.lcs.mit.edu/thomer/mit/multops_usenix2001.pdf)
- [8] <http://cat.ice.ntnu.edu.tw/tcpip/main.htm>
- [9] <http://www.sans.org>
- [10] <http://www.snort.org>
- [11] Gary C. Kessler , “Defenses Against Distributed Denial of Service Attacks”, November 29, 2000  
<http://www.sans.org/infosecFAQ/threats/DDoS.htm>
- [12] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson ,”Practical Support for IP Traceback”, ACM SIGCOMM, pp. 295-306, August, 2000

- [13] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, Diego Zamboni, “Analysis of A Denial of Service Attack on TCP”, Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on , 1997
- [14] AXENT Technology Ltd. , “Everything You Need to Know About Intrusion Detection”, 1999

