以 ICAS 提供雲內網路入侵偵測日誌分析

楊順發

國家高速網路與計算中心

OUTLINE

- Introduction
- Background
- Motivation
- Related Works
- System Architecture
- System Visualization Demo

INTRODUCTION

- **Benefit of Cloud Computing**
  - Reduced Cost, Increased Storage, Highly Automated, Flexibility, More Mobility, Allows IT to Shift Focus
- **All of Operation through The Network Connection**
- **Security is an important issue**
- **Goal**
  - IDS Log Cloud Analysis System (called ICAS)
  - Provide fast and high reliability of the system.

BACKGROUND

- Intrusion Detection System
- Cloud Computing
- Motivation

INTRUSION DETECTION SYSTEM

- **IDS is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.**
- **Two Different Ways of Detection Methods**
  - Anomaly Detection
  - Misuse Detection

CLOUD COMPUTING

- **New Concept, not a New Technology**
- **Classify:**
  - IaaS(Infrastructure as a Service)
  - PaaS(Platform as a service)
  - SaaS(Software as a service)

MOTIVATION

- Security is an important issue in cloud computing period.
- We have to solve and to improve the performance of analysis efficient by large-scale computing due to there are large-scale IDS log files.
- Traditional way: dynamic webpages and database.
- We used the algorithm of hadoop called MapReduce to improve the performance, and crate output view friendly.

RELATED WORKS

- Alert Correlation
- Existing IDS Types
- Hadoop

ALERT CORRELATION

- **Alert correlation is an analysis process that takes the alerts generated by IDS and creates reports under its surveillance network.**

EXISTING IDS TYPES

- **NIDS: To monitor network spigot and to detection exceptionally transmission behavior by connecting to network hubs or network switch**
- **HIDS: This is inseparable from operating system and to detect and monitor malicious actives such as system calls, file system changes, application logs.**

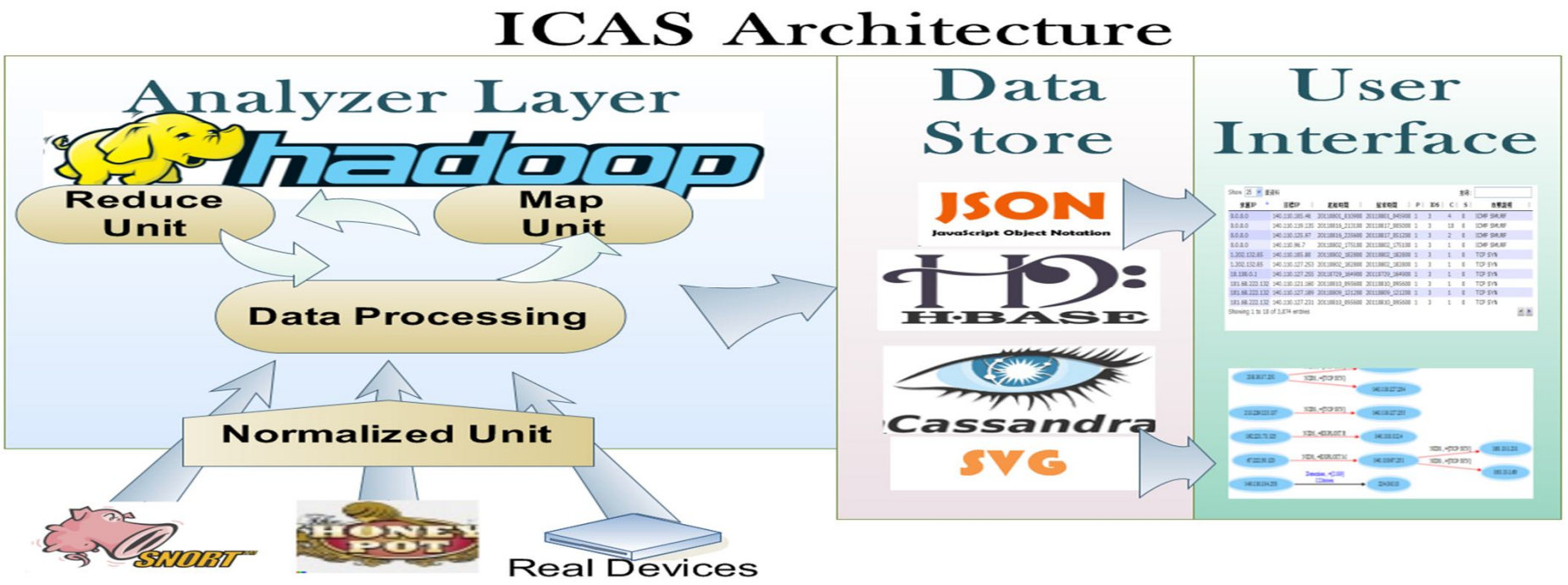
HADOOP

- Hadoop was inspired by Google's MapReduce and Google File System (GFS) papers.
- Hadoop is a powerful computing platforms, which is used to process large-scale computation and includes distributed file system.
- Enables applications to work with thousands of nodes and petabytes of data.

ALERT INTEGRATION PROCEDURE

- **System Architecture**
- **Analysis Format**
  - Input Format and Output Format
- **Integrating IDS into Cloud Computing Platforms**

SYSTEM ARCHITECTURE



ANALYSIS FORMAT

- **Snort**

  [**] [1:2189:3] BAD-TRAFFIC IP Proto 103 PIM [**]
  [Classification: Detection of a non-standard protocol or event] [Priority: 2]
  05/17-08:30:14.750704 140.110.138.253 -> 224.0.0.13
  PIM TTL:1 TOS:0xC0 ID:4076 IpLen:20 DgmLen:58
  [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0567][Xref => http://www.securityfocus.com/bid/8211]

- **IDP8200**

  Time Received ## Src Addr ## Dst Addr ## Action ## Protocol ## Dst Port ## interface ## Description ## Severity
  2003/8/11
  13:05,140.113.130.221,0.0.0.0,Accepted,TCP,65432,'interface=eth2',FTP: Format String in Command,Major

- **NK7Admin**

  NO. ## name ## from(address) ## to(address) ## start time ## total ## from(port) ## to(port)
  1,TCP SYN,60.173.26.116,140.110.127.253,2011/3/1
  14:41,1,6000,9415

INPUT FORMAT AND OUTPUT FORMAT

- **Output as <Key, Value> Pair**

Key:

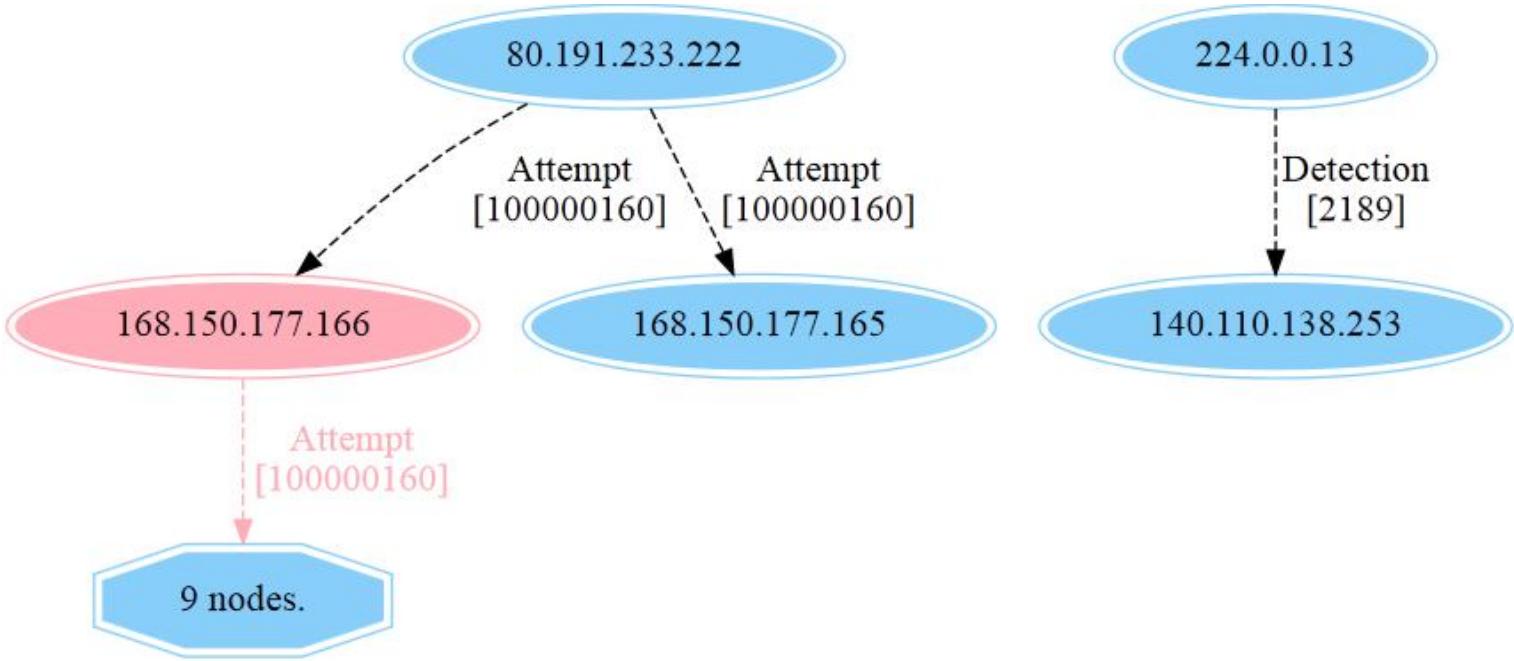
- <src_ip – dst_ip>

Value:

- <date @@ time @@ class_id @@ ids @@ s-id @@ priority @@ port @@ description>
- **ICAS will count these attack record as < *IDS Source; Alert Identification; Attack; Class; Severity(1~3); Date; Time; from(IP Addr.); to(IP Addr.); Port NO.*>**

SYSTEM VISUALIZATION DEMO

- **The Graph of ICAS Output**



DEMO WEBSITE

HTTP://CRAWLWEB2.NCHC.ORG.TW/ICAS-EN/INDEX.PHP

Explanation

Warning List

IDS means Intrusion Detection System, support as follows:

* snort = 1
* IDP8200 = 2
* NK7Admin = 3

P means priority, 1~3 , 1 is the most serious.

C means merge count

S means Snort Signature ID, for more detial please see http://www.snortid.com/ps : only Snort support this function

List

Show 25 筆資料 搜尋:

來源IP	目標IP	起始時間	結束時間	P	IDS	C	S	攻擊說明
0.0.0.0	140.110.105.46	20110801_010900	20110801_045900	1	3	4	0	ICMP SMURF
0.0.0.0	140.110.96.7	20110802_175100	20110802_175100	1	3	1	0	ICMP SMURF
1.202.132.85	140.110.105.80	20110802_182800	20110802_182800	1	3	1	0	TCP SYN
1.202.132.85	140.110.127.253	20110802_182800	20110802_182800	1	3	1	0	TCP SYN
10.100.0.1	140.110.127.255	20110729_164900	20110729_164900	1	3	1	0	TCP SYN
101.68.222.132	140.110.127.189	20110809_121200	20110809_121200	1	3	1	0	TCP SYN
108.59.3.28	140.110.117.141	20110729_131500	20110802_120600	1	3	2	0	VULN MS Windows SChannel Security Remote Code Execution
108.61.17.196	140.110.102.27	20110809_081700	20110809_081700	1	3	1	0	VULN MS Windows SChannel Security Remote Code Execution
109.0.0.0	140.110.111.125	20110730_132800	20110730_132800	1	3	3	0	ICMP SMURF

CONCLUSIONS

- Proposed IDS Log Cloud Analysis System
- The significant benefits to build IDS analysis system on Cloud platform are its scalability and reliability.
- Many aspects of this research need to be improved and expanded in the future.
- For further works, we will support more IDS type, and more clearly and friendly reports. Due to there are producing very huge IDS log files, we also need to improve the algorithm of ICAS for processing large-scale data.

THANK YOU!

Any Questions?

Shun-Fa Yang (shunfa@narl.nchc.org.tw)

Yao-Tsung Wang(jazz@narl.nchc.org.tw)