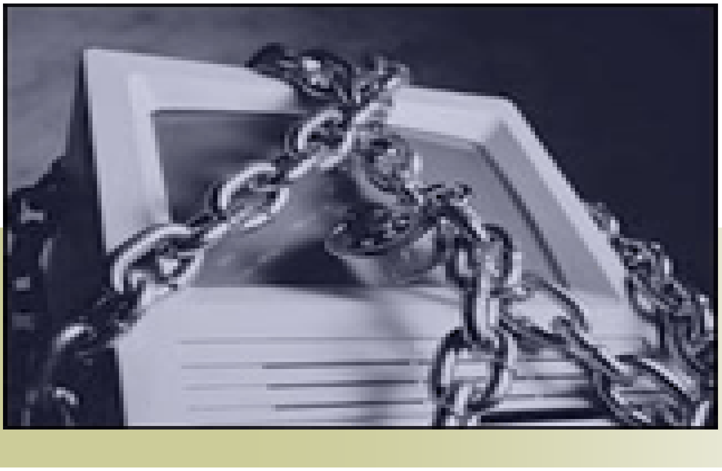

ANALYSIS ON IDS EVALUATION USING A QUANTITATIVE ASSESSMENT APPROACH

HATIM MOHAMAD TAHIR
NOORULSADIQIN AZBIYA YAACOB
SHAHRUDIN AWANG NOR
NOR IZZAH YAHYA

Computer Security Group
Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM, Kedah
MALAYSIA

OUTLINES

- INTRODUCTION
- PHASES OF THREAT
- AN IDEAL IDS REQUIREMENT
- RELATED WORK
- EVALUATING INTRUSION DETECTION SYSTEM
- RESULT
- CONCLUSION

INTRODUCTION

- IDS ARE PROLIFERATING THROUGHOUT CORPORATE, GOVERNMENT AND ACADEMIC COMPUTER NETWORKS SINCE THE GROWING NUMBER OF COMPUTER SECURITY INCIDENTS

- THE GOAL OF IDS IS TO IDENTIFY, PREFERABLY IN REAL TIME, UNAUTHORIZED USE, MISUSE AND ABUSE OF COMPUTER SYSTEMS BY BOTH SYSTEM INSIDERS AND EXTERNAL INFILTRATORS

- NOWADAYS, ID IS AN IMPORTANT TECHNOLOGY BUSINESS SECTOR AS WELL AS AN ACTIVE AREA OF RESEARCH

PHASES OF THREAT

Network attack is usually divided into three important phases (Carter, 2002):

- **FIRST PHASE**

Involves the setting of objective in performing an attack. As a rule, an attacker will determine one goal based on the reason to attack.

- **SECOND PHASE**

The second phase is reconnaissance or also known as information gathering. At this stage attackers would gather the network's data as much as possible in order to identify prime targets in the network.

- **THIRD PHASE**

After the collecting of information is complete, attackers will move on to the third phase that is attack. If the access to the system can be accomplished successfully, the main aim of the attacker will be made easier and any further attack would be continued from the computer that has been infiltrated

AN IDEAL IDS REQUIREMENT

Fyodor (2000) stated that an ideal IDS:

- Should Be Able To Detect, Report And Prevent A Wide Range Of Security Events
- Should Be Able To Perform Its Action In Real Time
- Resistant To Denial Of Service Attacks
- Detect Known And Unknown Intrusion Method
- Generate Zero Percent Of False Positives

RELATED WORK

Table 1: Characteristics of Past Intrusion Detection Evaluations

Studies	Evaluation Based on IDS Needs				Comments
	Accuracy	Performance	Completeness	Fault Tolerance	
Puketza,1994	Yes	Yes	Yes	No	Developing the methodology and software platform for IDS evaluation – Evaluate NSM (Network Security Monitor)
Debar et al,1998	Yes	Yes	Yes	Yes	Constructing IDS workbench to facilitate prototypes comparison developed by IBM Zurich
Lippman et al,2000	Yes	No	No	No	Evaluating IDS performance as supported by DARPA
Allessandri,2000	Yes	No	No	No	Developing method to combine IDS and reducing failure (work in progress)

RELATED WORK (cont..)

Studies	Evaluation Based on IDS Needs				Comments
	Accuracy	Performance	Completeness	Fault Tolerance	
Rossey et al,2001	No	No	No	No	Continuing efforts to overcome DARPA flaws, providing tools for IDS development and testing
Shipley and Mueller,2001	No	No	No	No	Comparison of nine commercial IDS products and one open source IDS
Mier Communications Inc. (personal company)	No	Yes	Yes – Load and vulnerability tests	Yes	Comparison of the IDS commercial product's effectiveness
NSS Report	Yes	Yes	Yes – Load test	No	Consumer report

RELATED WORK (cont..)

- Various projects have already made inroads into the field of testing IDSs.

- The eight previous works (Table 1) were the most important projects in this field. However, till now there are none standard benchmark that has been used for IDS evaluation testing; each with their own way.

- McHugh (2000) has critique the DARPA work on the appropriateness of the evaluation technique used and points out the shortcomings of the Lincoln Lab effort by giving some recommendations for activities related to evaluation.

- The recommendations cover the development of more appropriate measures of performance, better traffic characterization and validation, extension of the experiment to commercial systems and establishment of a canonical attack repository for future works.

EVALUATING IDS

- This study try to analyze the used of intrusion detection system (IDS) whether it can fulfill the identified IDS requirements by Porras and Valdes (1998) and Debar et al. (1999) which is used as predictable baseline in conducting some suggested experiment or test.

- The requirements are:

- Accuracy: Should IDS be able to detect many types of intrusions accurately?

- Performance: Should IDS function without monopolizing system resources such as main memory, CPU time and disk space?

- Completeness: Should stressful system conditions, such as a very high level of computing activity, not impair IDS function?

- Fault Tolerance: Should IDS completing all tests without a crash, lockup or noticeable performance degradation?

EVALUATING IDS (cont..)

OBJECTIVE	TESTS
1. Accuracy	Intrusion Identification Tests I) Basic Detection Test II) Normal User Test
2. Performance	Resource Usage Tests I) Disk Space Test
3. Completeness	Stress Tests I) Stress Test: High-Volume Sessions II) Stress Test: Intensity III) Stress Test: Load IV) Stress Test: Vulnerability
4. Fault tolerance	Fault tolerance test

RESULT (ACCURACY)

ATTACK CATEGORY	DETECTED	
	ISOLATED LAN (BASIC DETECTION TEST)	NETWORK (NORMAL USER TEST)
Application Bug	2	2
Backdoors	2	2
Distributed Attack	2	2
Denial of Service	2	2
Evasion	3	3
Informational	3	3
Mis-configuration	2	2
Malicious Data Input (Buffer Overflow)	3	3
Web-application-attack	0	1
Web-application-activity	0	4
Attempted-recon	0	6
Misc-activity	0	1
Not suspicious	0	1
Bad-unknown	0	1
TOTAL ATTACKS DETECTED	**19**	**33**

RESULT (ACCURACY)

- In normal user test, thirteen new alerts had occurred, while all attacks, which had successfully been detected in basic detection test, can also be verified in this test. New alerts that had been detected were analyzed to know whether it was the true signature detected or oppositely that is called false positive.

- After some initial investigation had been done, the false positive that occurred in the normal user test was the result of the students' activities themselves. This situation is known as the false positive because of the legitimate action has been detected as intrusion by the alert given.

RESULT (PERFORMANCE)

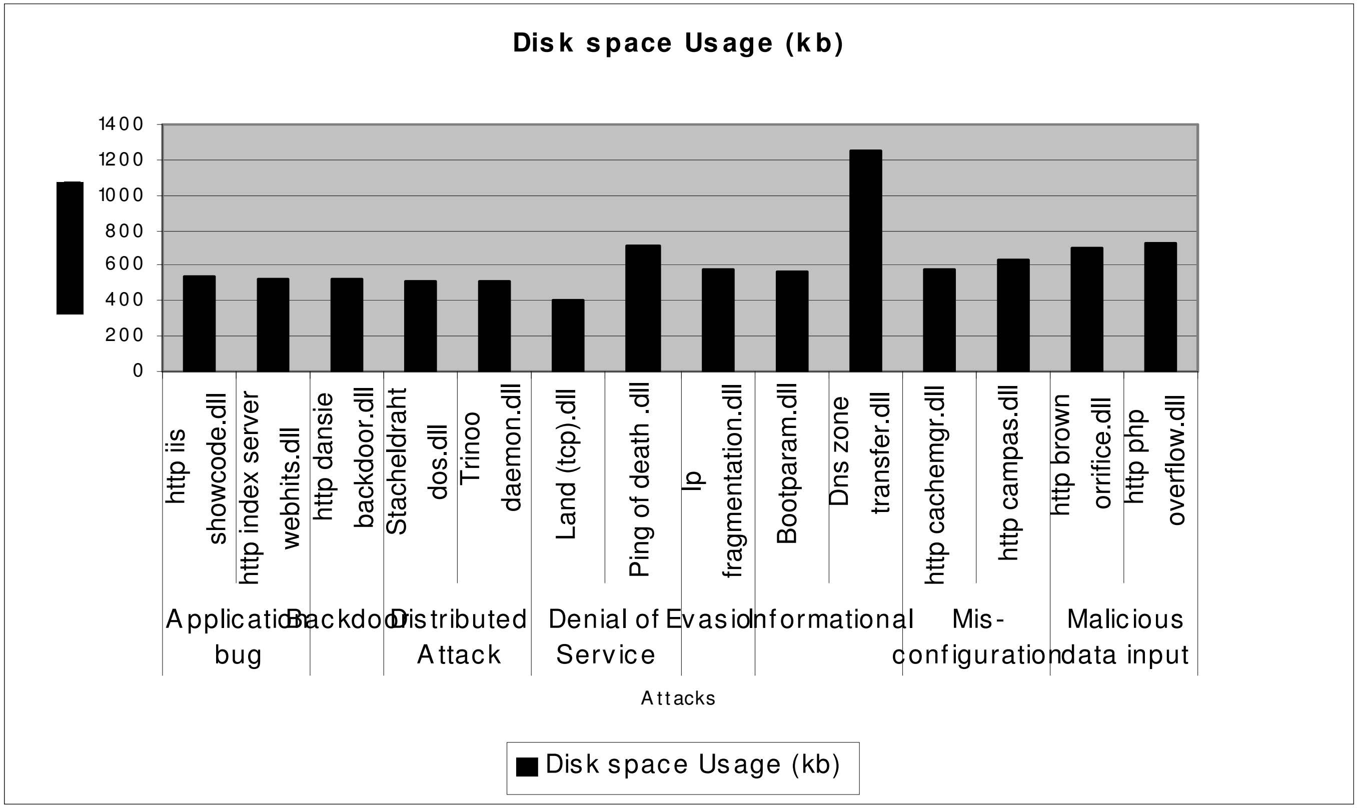

Figure 1: Disk Space Usae Graph by Eight Categories Attack

RESULT (PERFORMANCE)

- From the experiment that has been conducted, result shows ***Dns zone transfer*** **attack used the highest high storage and** ***Land (tcp)*** **attack got the lowest usage amongst all selected attacks launched for one-hour period time.**

- **IDS usage importantly depends on the disk storage in functioning stably.**

- **By default, log file is in the computer directory. The file is increasing rapidly when the attack detected by IDS is growing.**

- **The log file size will take a lot of disk space and increasingly using the disk space.**

RESULT (PERFORMANCE)

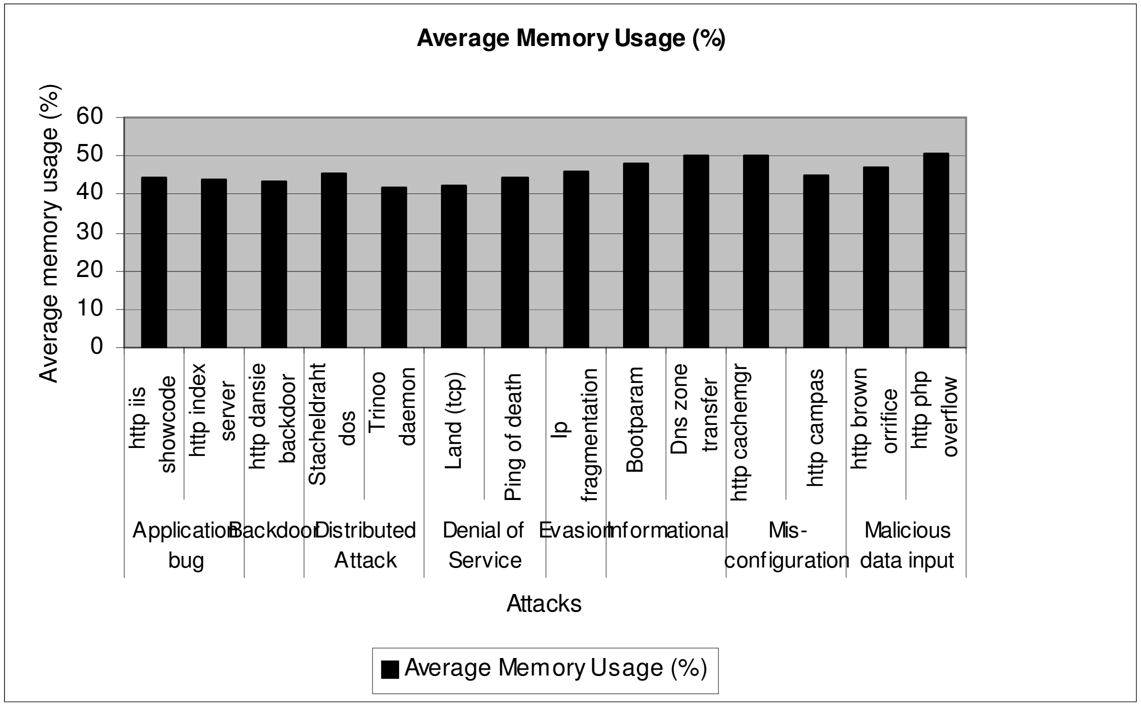

Figure 2: Average memory usage graph by eight categories attack

RESULT (PERFORMANCE)

- Overall, there are 3 attacks that score at least 50 per cent memory usage and for the remaining attack score between 40 to 50 per cent.
- Almost all the attack that have been launched, reached to half of maximum memory usage.
- Resource usages depend on how many data packet needed to process by IDS.
- As larger data packet have to be examined in order to match with the rule set, so as larger the resource is needed by IDS in doing detection.

RESULT (HIGH VOLUME SESSION-COMPLETENESS)

- In high volume session test, all attack can be detected with load from 1000 to 10000 KB volume of UDP packet not including distributed attack group that is *Stacheldraht dos* and *Trinoo daemon* attacks.
- It might be because the nature of the attack behavior itself. Both attacks are distributed denial of service (DOS) attack category.
- Distributed DOS is doing by intruding into several computers to launch attack in the target computer or network in the same time.
- The attack is hard to detect because the machine not only receive the packets from one computer but from several computer at the same time. The sheer numbers of IP addresses also, make it even much harder to filter and detect. Several packets might be able to escape from intrusion detection system.

RESULT (INTENSITY-COMPLETENESS)

- **Intensity test considered three changes factors; i) delay in seconds between sending attack; ii) delay in milliseconds between sending each packet and; iii) time to live (TTL).**

- **The result from intensity test shows that *IP fragmentation* attack cannot be detected by the IDS when the time to live is set to 0 while the delay between sending attack and each packet give influence to the time detection.**

- ***IP fragmentation* attack also cannot be detected when the three factors are set to 0.**

- **The result from intensity test shows that the technique used in launching attack might influence the alert generated. Therefore, the signature pattern for the attack is not static and different according to how the attack is launched.**

RESULT (LOAD-COMPLETENESS)

- The result from load test shows that IDS can detect less than 60% of the attack which has been launched when the computer resource usage exceed to maximum.
- This condition is called as false negative. False negative is when the attack cannot be detected by IDS and it will give a bad impact to overall system.
- Nevertheless, the inability to ascertain this attack is not linked to the characteristic of the attack but it is caused by maximum load stress resulting in the failure of IDS to perform efficiently.

RESULT (VULNERABILITY-COMPLETENESS)

- The results from vulnerability test demonstrate that IDS can still detect an intrusion in the required time allocated even though there is enormous amount of attack trying to damage the IDS itself.
- The observation done showed the increase of storage space, which has been used in three period intervals.
- This situation if left in a period of time is believed to cause IDS unable to function which consolidate the known fact that IDS failed to function when storage usage has reached its maximum.

RESULT (FAULT TOLERANCE)

- The requirement of fault tolerance is evaluated based on the experiment, which has been carried out, and the observation for all tests included intrusion identification test, resource usage test and stress test.
- IDS is able to diagnose all denials of service attacks that have been launched continuously for the period of one hour without encountering any problem.
- Nevertheless, IDS completes all tests with a lockup when the log file exceeded the file storage.
- Overall test shows that if the disk space is full, the IDS will stop respond to the attack launch. In order to solve this problem, the storage space should be unloaded without any reconfiguration on the IDS in order to enable it to function as usual.

CONCLUSION

- As computer systems and the Internet have grown in size, complexity and usage the demands placed upon those responsible for ensuring the continued operation and security of these systems have also grown.
- Due to the increasing attack techniques that continuously and widely expand from time to time, testing on IDS is needed to make sure that the IDS employed is functioning well.
- In this study, the evaluative set that has been constructed is used in designing test to evaluate IDS capability and in the same time revealing the IDS weaknesses for improvement.

THANK YOU