INTRUSION NOTIFICATION VIA SMS

By

AZIZ KASMIR MAT YUNOS

2003346265

A PROJECT PAPER SUBMITTED

IN PARTIAL FULFILMENT OF REQUIREMENT

BACHELOR OF SCIENCE (Hons.) IN DATA COMMUNICATION AND NETWORKING

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCE

MARA UNIVERSITY OF TECHNOLOGY

SHAH ALAM

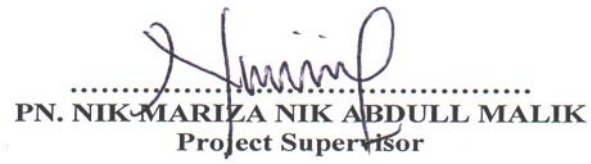
NOVEMBER 2006

INTRUSION NOTIFICATION VIA SMS

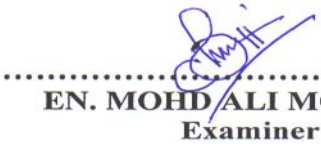
AZIZ KASMIR MAT YUNOS
2003346265

This project submitted to the
Faculty of Information Technology and Quantitative Science
MARA University of Technology
In partial fulfillment of requirement for the
BACHELOR OF SCIENCE (Hons.) In DATA COMMUNICATION AND NETWORKING

Approved By the Examining Committee:



PN. NIK MARIZA NIK ABDULL MALIK
Project Supervisor



EN. MOHD ALI MOHD ISA
Examiner

MARA UNIVERSITY OF TECHNOLOGY
SHAH ALAM

NOVEMBER 2006

CERTIFICATION OF ORIGINALITY

This is certified that I am responsible for the work submitted in this project that the original work is my own except as specified in the references and acknowledgement and that the original work contain herein have not been taken or done by unspecified sources of persons.

AZIZ KASMIR MAT YUNOS

ACKNOWLEDGEMENT

In the name of Allah, The Most Gracious, The Most Merciful, and Him alone are worthy of all praise.

It is not possible for me to acknowledge individually the debts that I owe to who had made their contribution in preparing and writing this research project proposal. I would like to thank many people who helped me

Special thanks go to my supervisor, Pn. Nik Mariza Nik Abdull Malik for her wonderful support, guidance and cooperation that had been given to me throughout the compilation of this project. I would also express my gratitute to Encik Adzhar Abdul Kadir who had been guiding the writing of this report from the beginning. Thank you to my examiner, Encik Mohd Ali Bin Mohd Isa for his guidance and support.

I would like to thank my family and two my best friend Iqbal and Shahariz Aziz for their deepest concern and investment during the course of this project. All of you are my strength and thanks for everything.

I would like to extend my sincere thanks to my fellow classmates and housemates, dedicated CTN lecturers and the others for contributing and supporting me directly and indirectly. Thanks for your support, comments and advice. Finally, thank you to all parties for participation and commitment in making this project successful.

Thank you, may Allah SWT bless all of you.

ABSTRACT

This project is aimed to have an NIDS (Snort) intrusion notification via SMS in the real time. In order to achieve the project goals, the logdog Perl script have to be added new configuration to support snort log parsing and send SMS to Gnokii SMS gateway. Snort rule also have to be reconfigure to minimize SMS sent when intrusion detected. Beside that Bluetooth configuration also need to be tweak so it supports Nokia 6280 mobile phone that work as GSM modem. The outcome of this project is a reliable NDIS Intrusion Notification via SMS that support real time intrusion detection alert notification.

Table of Content

1.0 Introduction

1.1 Project Introduction

Defeating malicious attempts to attack any network is difficult. The attacker has all the advantage of stealth, surprise, tenacity, and often even skill. Defending a network becomes even more difficult as the scale of the network increases. Today's fast-paced information intensive society requires that every member of an organization have a connection to the internet. This is true for small families to the medium sized business of a few hundred employees to the largest government organizations employing millions of people. Each of these connected computers provides an opportunity for an attacker to sneak into the network to wreck havoc or steal vital proprietary or classified information.

IDS system is required here to detect attacks against computer network and notify us when the attacks occur. An Intrusion Detection System (IDS) is the high-tech equivalent of a burglar alarm. A burglar alarm configured to monitor access points, hostile activities, and known intruders. The simplest way to define IDS might be to describe it as a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers, and other network devices. IDS can provide an after-the-attack audit trail for seeing how far an attacker got, and where it came from.

Snort is now the most widely deployed IDS systems in the world and SNORT IDS will be used for the project. Snort is an open source *Network Intrusion Detection System*

(NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network. There is also host-based intrusion detection systems, which are installed on a particular host and detect attacks targeted to that host only.

The monitoring of intrusion detection in the network taken so much time of the administrator and it required the person to have 24 hour availability in front of the computer. To minimize it, SMS alert systems will be used to minimize the time of administrator availability in front of the computer to monitor intrusion. This SMS system will be interfacing with Snort base rule to log alert process to send an SMS alert to administrator. In order for this Intrusions Notification via SMS to be implemented, many methods will be used to have this alert system.

1.2 Problem Statement

So much time taken to monitor the intrusion detection in the network by administrator with current setup of monitoring the intrusion alert, but many of systems administrators are assigned to manage various IT related task/job in the company. The using of e-mail systems to alert the responsible person also created the same problem where it still took the time of the system administrator. This is because they still have to be in front of the computer to get the alerts. This showed how slow the action taken with alerts/threat in real-time.

For ease of systems administrator, the researcher tries to eliminate this problem by having the Intrusions Notification via SMS. The transformation to the new will be system hopefully will give benefit for systems administrator. With the SMS alert system hopefully it can reduce time required by systems administrator to monitor intrusion/threat in the network and also give systems administrator enough time to do multitasking job function in networking environment.

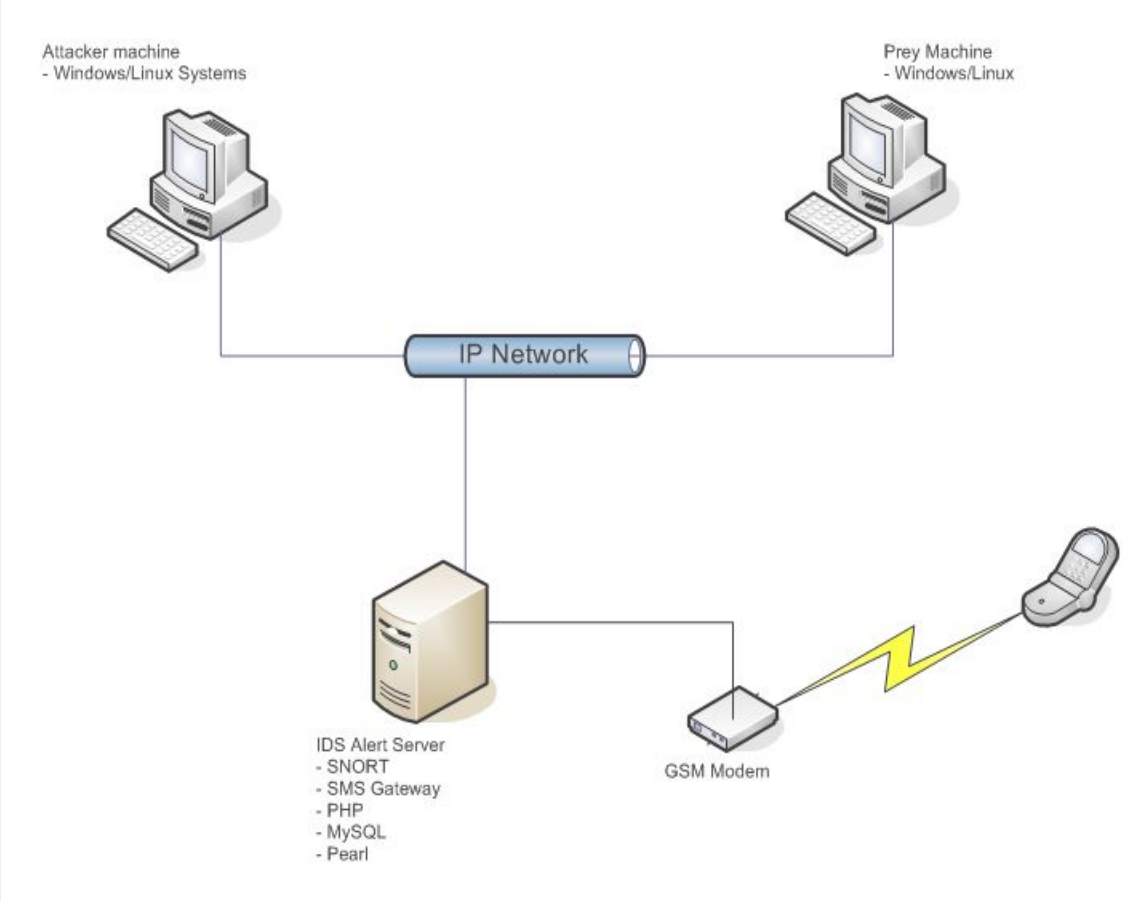
1.3 Project Objective

The objective of this project is to have real time IDS alert systems by using SMS gateway (GNOKII) interface with Snort (IDS tool) to send intrusion alert to the administrator using PERL script. This systems can reduce the require time usage by administrator to monitor the intrusion in the network. With growing number of intrusion and attack by hacker in computer networking, the knowledge of IDS is must for future systems administrator and this study also give the opportunity and benefit for researcher to study IDS in detail and how to manage future networking challenges.

1.4 Project Scope

The project is tested in simulation of 3 computers in small network by using 1 computer notebook installed with Windows XP PRO and VMWARE Workstation 5.0. Host machine Windows XP will host the other 2 computer by using VMWARE. This virtual

machine will be installed with KUBUNTU Linux and another with UBUNTU Linux. The Windows XP systems will be targeted machine and UBUNTU Linux virtual machine will be the attacker in this simulation of IDS systems setup. KUBUNTU Linux virtual machine is used for IDS server where it connected to GSM Modem (Nokia 6280) and PERL script to send the SMS alert to administrator mobile phone. The attacker computer will have *nmap* and other attacking tools used for scanning and attacked the victim computer.



Proposed Intrusion Notification via SMS Simulation diagram

1.5 Project Significance

Time factor is the most important value in working environment. Job as systems administrator required the person to do multitasking job in the networking environments. Furthermore most of the companies treat the systems administrator jobs as expenses to the company. To have systems administrator to do multitasking job in the networking environment is a must. This system will reduce the time of the systems administrator had to monitor intrusion detection job, which this alert system will give administrator a real-time alert on intrusion in the network.

2.0 Literature Review

2.1 Intrusion Detection Systems Overview

An intrusion in computer networking terms is defined as someone (hacker, cracker) attempting to bypass security protocols and infiltrate a network system. The motivation behind this could be something as sinister as stealing confidential data, misusing e-mail for spam, or any number of things for which a system administrator could be held responsible. As shown by the February 2000 DOS (Denial of Service) attacks against the major Internet service providers, the frequency of security incidents are increasing. Even more alarming is the evidence that such attacks are becoming much more intelligent, subversive, and harmful. It has become certain that anyone responsible for a network

with an Internet presence is now a potential target, and intrusion detection systems are quickly becoming a necessity.

An intrusion detection system (IDS) is a system designed to systematically detect host attacks on a network. These systems provide a secondary, passive level of security by providing the administrator with critical information about intrusion attempts.

In actuality, the IDS simply alert the system administrators upon detection of computer attacks or computer misuse. Often IDS is used in conjunction with a firewall whose sole aim (through packet analysis) is to control the flow of *datagrams* into and out of a network. *Datagrams* are simply the packet bundles of information that computer systems use to communicate with each other over the network. Typically IDS are not intended to block or actively counter attacks, but some newer systems have an active capacity for dealing with threats. Indeed, a very knowledgeable human being should be watching and making value judgments on the ‘alerts’ that the IDS has presented him or her with. While firewalls can be thought of as a border or security perimeter, IDS functions to detect whether that border has been breached. Under no circumstances does an IDS guarantee security, but with proper policies, authentications, and access control, some measure of security can be attained.

2.1.1 Operation and Function of IDS

Intrusion detection systems serve three essential security functions: they strive to monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. Intrusion detection systems can use rule-based policies that match packets or analysis of user behavior with predetermined security events. Typically, IDS send out alerts if they detect one of these security incidents.

Some IDS not only send alerts but also respond to the threat of an event. These responses usually take the form of removing a user, disabling user accounts, launching scripts, and dropping packets. These IDS are in a special class of intrusion systems called IPS or Intrusion Prevention Systems. It is estimated that up to 85% of security incidents on networks come from inside the network firewall. The other 15% or more come from outside in the form of denial of service attacks, buffer overflows and the like. Some of the most inventive attacks are known as Trojan Horses. These are destructive programs masquerading as harmless applications such as e-mail attachments promising to rid your computer of viruses but instead introducing its own virus onto your computer. Currently, intrusion detection systems are the only tools that system administrators possess for detecting and responding to intrusions once the attacker has bypassed the firewall and has gained access to the network. There are four major IDS techniques used to detect intruders: **anomaly detection, misuse (or signature) detection, target monitoring,** and **stealth probes**.

2.1.2 Anomaly Detection

Anomaly detection searches out abnormal patterns of behavior, where an IDS establishes what is known as a "baseline of normal usage," and then any deviation from that baseline is marked as a possible security problem. For example, a computer that has been logged into at 3 a.m. from an office that closes at 6 p.m. should certainly cause a behavioral alert warning. Another instance might be an employee working in the web development group who suddenly takes great interest in accounting software. This would also constitute a standard deviation in baseline normal behavior.

2.1.3 Signature Detection

Signature detection uses specific patterns to detect similar intrusion attacks. Network intrusion detection systems use signatures or partial strings that match parts of the network packet itself. Once the strings are matched, notification is sent to the proper authorities and the incident is logged. These intrusion attempts mark signatures already programmed into the signature database that match parts of the network packet itself. Once the IDS match a string, it responds by sending the System Administrator an alert. For instance, if several ‘backdoor attempts’ are sent from a specific host and the system administrator responded properly, eventually it would be determined, if the computer was an inside host, that a hacker was attempting to infiltrate the computer.

2.1.4 Target Monitoring

Target monitoring searches for modifications of specific files and often cryptographic caches are calculated and compared to new caches of specific files at regular intervals. If these fail to match, then the IDS consider an intrusion to have occurred. An excellent example of target or integrity monitoring is the Tripwire product (*www.tripwire.com*). Tripwire monitors the following attributes:

• File additions, deletions, or modifications

• Flags on files (hidden read-only)

• Access times

• Write times

• Change times

• File size

• Hash checking

2.1.5 Stealth Probes

Stealth probes are designed to detect attackers who carry out their attack over prolonged periods of time. These hackers, or crackers, test system vulnerabilities and try to open ports, and after a lengthy period of time, actually begin their attacks. These attacks are very difficult to detect. Stealth probes use wide area sampling and try to correlate port scans with later attacks from the same IP numbers.

Although many versions of IDS exist, there are some terms and general definitions common to all. These call an **alert** a true alarm, one which identifies that the system in question has been significantly attacked. This means that a hacker has made contact or attempted to make contact with vulnerability inside the network area. A false positive is an alarm generated for conditions that do not exist or are no threat inside our network environment. A false negative occurs when the IDS does not alert when an alert worthy condition has happened. Noise occurs when an IDS alerts on conditions that are either none threatening or truly not applicable to the network sites which are being monitored; however, the IDS was correct in diagnosing these.

2.2 Introduction to Intrusion Detection Systems

There are two classes of intrusion detection systems: host based and network based. Each class has distinct advantages and disadvantages. Host based IDS survey data on individual nodes of a network, whereas network based IDS examine those packets which are exchanged between network nodes.

2.2.1 Host-based IDS

Host based intrusion detection systems can be broken down in roughly four types. These include log monitors, integrity monitors, signature scanners and anomaly detectors.

Logfile monitors try to detect intrusions by parsing system event logs. Target monitors, signature scanners, and anomaly detectors have already been discussed.

Host based IDS (HIDS) analyze datagrams which may originate from computers which host services. A good example of this would be a web server. Once the data is captured, the analysis may take place on the host or node or on an analysis machine. One type of HIDS is a program which constantly receives applications or operating system audit logs. These programs 'live' inside a trusted domain within the network and have been proven to be excellent detection devices, being close to network authenticated users. They are fast to respond and usually accurate in detecting unauthorized activity because they are right at the source.

The disadvantage to host based systems is the cumbersome administration and logging attempts made by these programs. If there are several thousand nodes on a large network with each node having its own HIDS, the likelihood of effective and efficient system administration for each of these programs would be impractical and nearly impossible. Also, if an intruder could disable the program or the data collection by the program on any of those given nodes, then the IDS would be completely ineffective in that circumstance. The alternative to a HIDS is a network based IDS (NIDS), which monitors data traffic throughout the network as opposed to residing on a single machine.

2.2.2 Network-Based Intrusion Detection Systems

The second class of intrusion detection systems is comprised of network based IDS (NIDS). Network based detection analyzes datagrams traveling over the entire network or switched sections of the entire network. Network packets are analyzed, sometimes compared with pre-stated rules, and then checked for veracity of their nature, whether harmful or benign. The primary technique employed by NIDS is packet sniffing. This approach pulls data from inside certain protocol packets and matches this data with predetermined accepted packet structure.

Network based systems are more effective than their host based counterparts at detecting unauthorized outsider access and denial of service or bandwidth theft. However, NIDS do have certain drawbacks, such as a difficulty in analyzing certain packets such as encrypted packet payloads, Unicode formatted packets, high-speed networks, highly switched networks, or any other packet formatted in a way which would make it impossible for a program to match predetermined signatures.

2.2.3 Advantages of monitoring Network Traffic

There exist many different operating system platforms, and hence, host-based systems have only been used on a single operating system at one time. On the other hand, network protocols like TCP/IP, UDP/IP are standard across most major operating system

platforms. By using these network standards, the network-based IDS can monitor a heterogeneous set of hosts and operating systems simultaneously.

Second, audit trails are often not available in a timely fashion. Some IDSs are designed to perform their analysis on a separate host, so the audit logs must be transferred from the source host to a different machine for data analysis. Furthermore, the operating system can often delay the writing of audit logs by several minutes. The broadcast nature of a LAN, however, gives the network-based IDS nearly-instant access to all data as soon as this data is transmitted on the network. It is then possible to immediately start the attack detection process.

Third, the audit trails are often vulnerable. In some past incidents, the intruders have turned off audit daemons or modified the audit trail. This action can either prevent the detection of the intrusion, or it can remove the capability to perform accountability and damage control. The network-based IDS, on the other hand, passively listen to the network, and are therefore logically protected from subversion. Since the IDS is invisible to the intruder, it cannot be turned off (assuming it is physically secured), and the data it collects cannot be modified.

Fourth, the collection of audit trails degrades the performance of a machine being monitored. Unless audit trails are being used for accounting purposes, system administrators often turn off auditing. If analysis of these audit logs is also to be performed on the host, added degradation will occur. If the audit logs are transferred

across a network or a communication channel to a separate host for analysis, loss of network bandwidth may discourage administrators from using such IDS. The alternative, namely, network-based IDS, will not degrade the performance of the hosts being monitored. The monitored hosts are not aware of the IDS, so the effectiveness of the IDS is not dependent on the system administrator's configuration of the monitored hosts.

And, finally, many of the more seriously documented cases of computer intrusions have utilized a network at some point during the intrusion. i.e., the intruder was physically separated from the target. With the continued proliferation of networks and interconnectivity, the use of networks in attacks will only increase. Furthermore, the network itself, being an important component of a computing environment, can be the object of an attack. The IDS can take advantage of the increase of network usage to protect the hosts attached to the networks. It can monitor attacks launched against the network itself, an attack that host-based audit trail analyzers would probably miss.

2.3 Hacker Methodology

This methodology is followed by all attackers, regardless of their skill, specific attack, or stated goal. In order to clarify the methodology, an illustration of the process a thief goes through while trying to steal jewels from a safe inside a house will be presented.

Step 1: Before a thief can steal anything he/she has to know where it is located. This requires some sort of surveillance of the house where the safe is located, including

activities like finding the house on a map, driving past the house, and taking pictures at different times of the day and week in order to understand as much as possible about the target. The thief's main purpose is to find a weakness in the house's defense. In a similar manner all network attackers must first find the computer they are trying to attack through the network before they can actually launch an attack. This is accomplished in the cyber world through network probing and scanning. Basically this entails sending out specifically formatted datagrams (like a SYN scan) to elicit a response from the targeted host and reveal the existence of some vulnerable piece of software.

Step 2: The next step a thief takes after he has finished his surveillance is to actually make an initial penetration into the house. For instance the thief may have discovered that there is no alarm on the rear window over the garage. To break into the house the thief will first break the window and get inside the house. Likewise our cyber-attacker must select an exploit from his bag of tricks and execute it against the victim host in an effort to establish a foothold inside the defensive perimeter. An example might be any of the recent Internet Information Server (IIS) buffer overflow vulnerabilities published in regard to Microsoft's web server. This exploit will typically only grant the attacker user-level access to the host.

Step 3: Once the thief has made it into the house he must now locate the safe and penetrate it in order to acquire the jewels that they were after in the first place. In the cyber world, the jewels of a host are typically protected by the root or administrator account. For an attacker to gain access to these jewels they must execute further