INTRUSION DEECTION SYSTEM using Sax 2.0 and wireshark 1.2.2

Faisal Mahmood

This document present in-depth knowledge of the Intrusion, various tools for intrusion detection, ways to prevent intrusion, project execution scheme, selecting the tools for project and learning from the project

Supervisor Dr. Akshai Aggarwal
Course CS 0360564
Assignment 1(mahmood1@uwindsor.ca)

10/6/2009

TABLE OF CONTENTS

INTRODUCTION

1.1 WHAT IS INTRUSION

There are quite a few factors that dictate how safe the data is on your computer. In defining "safety", we can either talk about it being safe from virus attack, safe from system damage, or safe from intrusion.

Intrusion, the act of someone that you don't know, who gains access to your computer without your permission, is on the rise. This is really a big concern and bad news for computer users as they always want to make it sure that their important data is safe from intruders.
The good news is that the vast majority of hackers are not sophisticated enough to get into your system if you employ a few precautions.

1.2 WHY INTRUSION IS DONE

Million dollar question …….*What hackers are looking for*
Honestly... there are no hackers out there that are looking to steal your latest great novel, your tax records, or even your latest digital pictures of the grandkids.
In fact, if you are like 99.9% of Computer users, there is nothing at all on your computer that a stranger would really be interested in. You may now want certain things to be available to the public, but that doesn't infer that anyone else has any interest.

Hackers are more interested in gaining access to your computer and using it for other purposes.
If a hacker can gain access and use your Internet access, then they can use your machine to launch other attacks on other computers and keep themselves pretty well hidden.

There are certain applications that take days to months to run a series of processes on even the fastest computer. But if a hacker can gain access to 1000 computers and utilize their combined processing power, a process that would take a month on a single computer could complete the operation in less than an hour.

Hackers have control of thousands of machine and can use them any time for their attacks. We experience many such events almost daily. Recent one was on Twitter, yahoo mail server and also on White House official web site.

Mostly intrusion is to retrieve the special data from the system or make the availability of any service difficult or completely shutdown. Big Ecommerce businesses portals suffer the most in the sense of revenue lose for those types of intrusion like amazon.com experienced recently.
Some time break-in by an unauthorized person may be an embarrassment that undermine the confidence that others have in the organization or name. Recent example is broken in by Chinese intruder in White House official web site.

Many underground hidden markets are actively involved in selling and purchasing hacked systems by the hackers so that they can be used by Intruders anytime for launching a specific attack on a specific day and time.

1.3 WAYS TO MINIMIZE THE INTRUSION

As I mentioned before that the good news is that the vast majority of hackers are not sophisticated enough to get into your system if you employ a few precautions. Some of them on regular basis and some of them after Intrusion are detected.

Keeping the computer up to date is not as difficult and complex as it sounds. Most of the updates are done over the internet.

Updating the Operating system regardless of what operating system is being used on the computer, if it is a Microsoft system such as Windows 95, Windows 98, Windows ME, Windows 2000, or Windows XP, Microsoft has an online utility that allows you to upgrade your system at no charge to you.

In fact, you don't even have to know what operating system (or OS) you are using to take advantage of this capability.

The later operating systems have better security built into them than the earlier ones, but all will be able to access the online patches that Microsoft offers. To update your Microsoft operating system, simply go *to http://windowsupdate.microsoft.com* and click on "Product Updates".
Follow the instructions and Microsoft will not only determine what operating system you are using, it will find out what security holes you have in your OS and will automatically download and install those patches for you. You will probably have to restart your machine as soon as that is done. *Simple and easy….isn't it ?*

Firewalls regardless of which internet service provider (ISP) you use (AOL, MSN, Prodigy, cable access or DSL Company) you should also install a firewall. Some internet service providers claim that they have a firewall built in, but the ones that I have seen are very ineffective if they are there at all.

Simply put, a firewall is a piece of software that stops intruders from accessing your computer. It sets up rules that allow you to access the Internet, but doesn't allow others to access your computer from the outside.

There are several great firewalls out there right now. Some are free, but for the sake of computer security, it's probably best to go the route of a known package that you pay for. For the money, I recommend Norton's Internet Security, available from Symantec.

You can download it if you want and are familiar with download procedures, but I highly recommend that you purchase the CD version from your local computer store and install it through your CD drive. In Windsor Futureshop and Bestbuy sell this product.
For about $60, you can get your computer up to speed and give it a very decent level of security. *Inexpensive …isn't it*

Intrusion by trojans and other funky animals comes from the inside out. If you have accidentally downloaded a virus or someone has gained access to your machine, it is possible that you have a Trojan on your machine.

A Trojan is aptly named because much like the stories of Homer, the Trojan is surreptitiously put onto your computer and then it acts behinds the scenes.
Once in place, the Trojan can carry on all sorts of activities including sending information out of your computer or creating a hole in a firewall that allows someone else to have outside access to it. Filling up those holes is very important to control and eliminate the intrusion.

Trojans can be a little tricky to get rid of. But once they are found, they are generally pretty easy to wipe out... *sneaky and nasty but not very strong*.

Antivirus programs can often find and eliminate viruses and Trojans. Various antivirus softwares are available in the market to eliminate the torjans. Some antivirus slows the performance of the system. One has to balance between compromising the speed and security of the system.

1.4 HOW INTRUSION DETECTION SYSTEM WORKS

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

An IDS can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.
Intrusion detection can be perform by implementing some important tasks on the host computer and network itself like real time traffic analysis and packet login on the IP networks. Protocol analysis, content searching, content matching and detecting variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Intrusion detection systems monitor and help eliminate unauthorized access to computers and security threats such as, packet sniffers, exploits, and denial of service (DoS) attacks. An intrusion detection system can monitor your computer or network for suspicious activity and alert you when something has been detected. This type of computer protection is valuable against new exploits and malicious software that have not yet been identified by antivirus vendors. This early warning system is used by corporations with large networks and can also be used on personal computers at home.

A **network intrusion detection system** (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.
A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. If, for example, a large number of TCP connection requests to a very large number of different ports are observed, one could assume that there is someone conducting a port scan of some or all of the computers in the network. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection systems does.
A NIDS is not limited to inspecting incoming network traffic only. Often valuable information about an ongoing intrusion can be learned from outgoing or local traffic as well. Some attacks might even be staged from the inside of the monitored network or network segment, and are therefore not regarded as incoming traffic at all.
Often, network intrusion detection systems work with other systems as well. They can for example update some firewalls' blacklist with the IP addresses of computers used by (suspected) crackers or hackers.

There are different types of Intrusion detection systems some of them are
Network intrusion detection system (NIDS)
Protocol-based intrusion detection system (PIDS)
Application protocol-based intrusion detection system (APIDS)
Host-based intrusion detection system (HIDS)
Hybrid intrusion detection system

1.5 INTRUSION DETECTION SYSTEM TERMINOLOGY

Intrusion detection systems use following terminologies to define the state
Alert/Alarm- A signal suggesting a system has been or is being attacked.
True attack stimulus- An event that triggers an IDS to produce an alarm and react as though a real attack were in progress
False attack stimulus- The event signaling an IDS to produce an alarm when no attack has taken place.
False (False Positive)- An alert or alarm that is triggered when no actual attack has taken place.
False negative- A failure of an IDS to detect an actual attack.
Noise- Data or interference that can trigger a false positive.
Site policy- Guidelines within an organization that control the rules and configurations of an IDS.
Site policy awareness- The ability an IDS has to dynamically change its rules and configurations in response to changing environmental activity.
Confidence value- A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack.
Alarm filtering- The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.

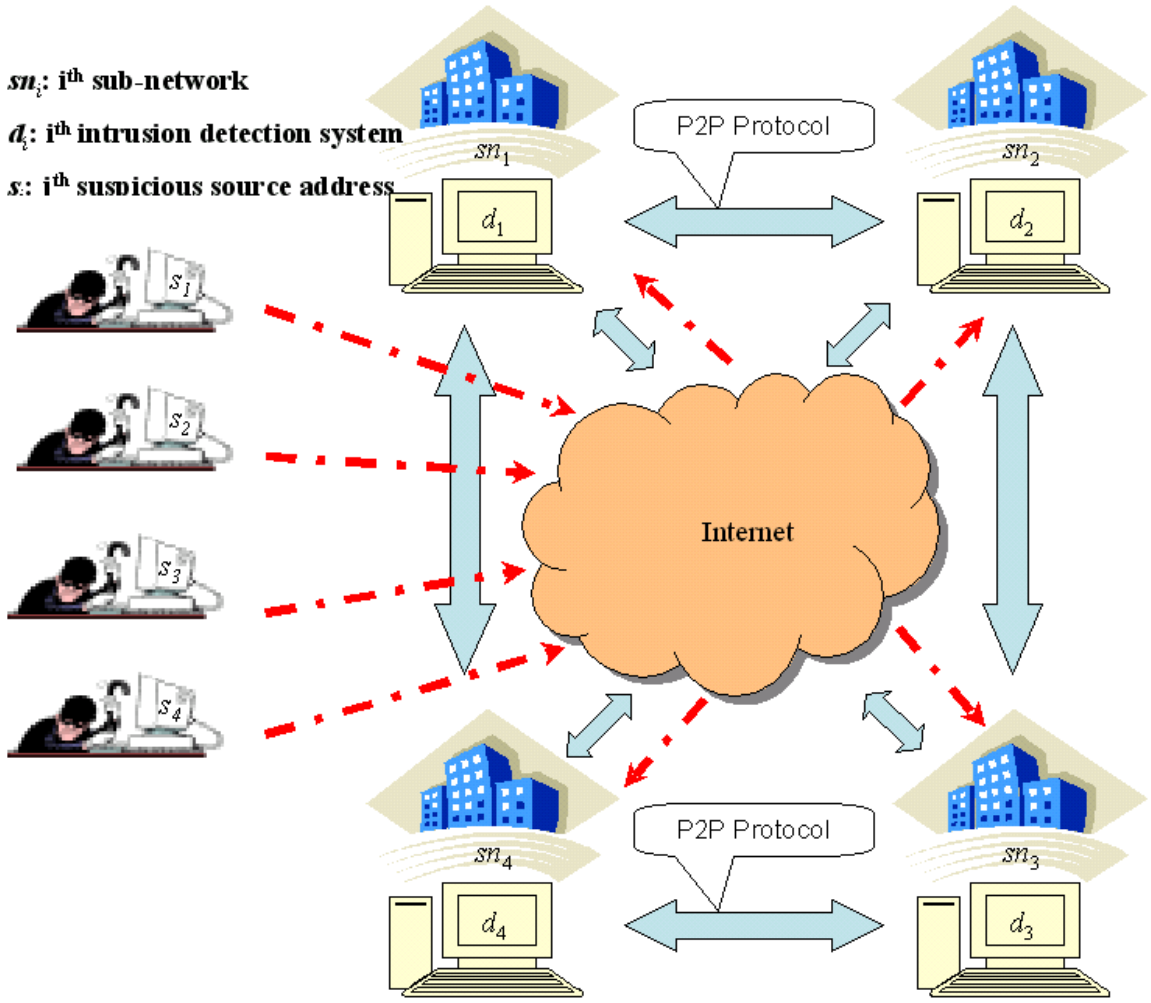


Fig. 1: An example collaborative intrusion detection system with four peers

PROJECT

2.1 DISCRIPTION OF THE PROJECT

My main project will be to detect the intrusion on the network. I will generate attack on one computer and will detect the intrusion on the other computer. As this is the learning project, I will use two or more computers, connect them and will perform the project on learning basis. I will install and use the free program in order to get a better understanding of how it works.

I will monitor the computers internet activity and try to stop any port scanning that may be happening. I will use the information gathered to build a good security profile for the computer which will give me a list of security settings that make the computer as safe as possible.

This goal of the project is to learn a new system and be able to use it in a real world setting. In this case I will be protecting a personal computer using a host based intrusion detection system.

2.2 ISSUES TO BE IDENTIFIED AND DISCUSSED

The main issue for this project is to check the host network for vulnerabilities and signs of hacker activity. The security issues involved are real world threats such as port scanning and probing attacks. The host machine will be connected to the internet and represents the typical home user machine.

I will monitor network traffic coming into the host machine and keep of all the traffic the host machine has received.

2.3 FOCUS IN THE PROJECT

By the end of this project I hope to have a security policy that will harden a home user system against intrusion. I will monitor network traffic coming into the host machine and keep a log of all the traffic the host machine has received. This project will monitor HTTP requests and check for FTP or TFTP transfers on the host machine. Worms like to use FTP or TFTP ports to download and send copies of it to other machines connected on the network. I will record what IP addresses that are requesting information and trying to establish connections with the host machine.

After Sax2 and Snort (selected tools) have identified threats or vulnerabilities I will take the correct preventive measures to fix the threat or vulnerability.

My baseline will be the monitored packet traffic before taking any preventive action. Then after the preventive step I will monitor packet traffic to see if Sax2 is catching suspicious behavior like it is suppose to.

Sax2 allows for customizable security policies and gives network traffic statistics. These capabilities along with computer generated audits will give me real-time response and accurate information of network activity.

The goal is to stop scanning and probing attacks at the firewall and catch any stealthy attacks with the intrusion detection system to give me defense in depth.

TOOLS AND SOFTWARE

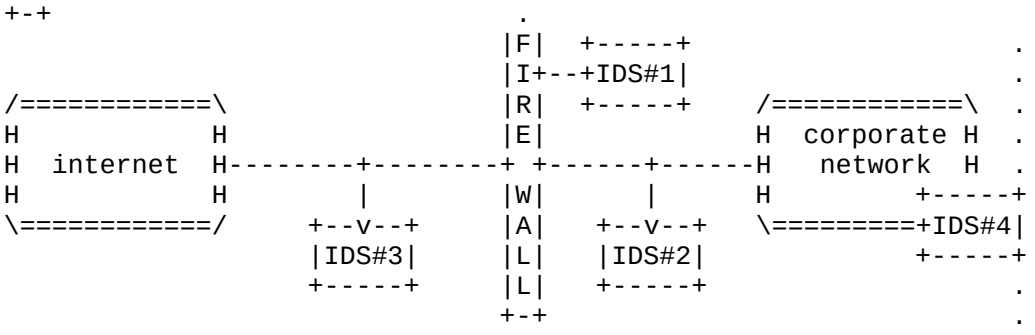
3.1 AVAILABE TOOLS FOR INTRUSION DETECTION SYSTEMS

Many tools and packages available online to detect the intrusion. Most of the tools are not free of cost. The normal price range is from $ 520 to $ 800 for one year subscription for the Intrusion tool.

Some famous and widely used Intrusion detection tools are

SNORT every one's favorite open source ID's
OSSEC HIDS An Open Source Host-based Intrusion Detection System
BASE The Basic Analysis and Security Engine
Sguil The Analyst Console for Network Security Monitoring
Netcat The network Swiss army knife
Metasploit Framework : Hack the Planet
Kismet : A powerful wireless sniffer
Hping2 : A network probing utility like ping on steroids
Tcpdump : The classic sniffer for network monitoring and data acquisition

- **Sax2 Intrusion detection** and prevention system (IDS)
- **Wireshark** fantastic open source network protocol analyzer for Unix and Windows (Selected tools for the Project1)



IDS to secure the corporate network

3.2 INTRUDUCTION TO THE SELECTED TOOL

Intrusion Detection System – Sax2

Ax3soft Sax2 is a professional intrusion detection and prevention system that performs real-time packet capturing, 24/7 network monitoring, advanced protocol analyzing and automatic expert detection.

By giving insights into all of your network's operations, Sax2 makes it easy to isolate and solve network problems, identify network bottleneck and bandwidth use, detect network vulnerabilities

and discovered the network whether there is a breach of security strategy and the signs of being attacked in the network of hazard, and then intercept and stop before their invasion.

Network administrators can directly monitor http requests, email messages, ftp transfers, as well as real-time activities and message details for the two popular instant messengers: MSN and QQ. Sax2 is designed to be used by both IT professionals and novice users.

Problems are clearly identified, and solutions are suggested in understandable terms. Whether you're a network administrator who needs to identify, diagnose, and solve network problems quickly, an IT professional who wants to monitor user activities on the network, a security manager who needs to ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients, Sax2 has the tools that you need.

Main Functions

1.Intrusion Detection and Prevention
2.Conduct of Audits
3.Traffic Statistics
4.Customize Security Policy
5.Real-Time Alert and Response

A network based Intrusion Detection System, which also enables a user to prevent intrusions through a host of useful tools.

Features: Sax2 is a mainly an Intrusion Detection System (IDS). To this end Sax2 performs advanced real time packet capturing functions, advanced protocol analysis, 24x7 network monitoring, and Expert detection.

It is a network based IDS: it collects, filters and analyzes all traffic that passes through a given network location. A single Sax2 monitor, appropriately placed (example: on a gateway) can provide IDS and intrusion prevention services for the entire network at a local site. Intrusion detection and prevention is done through the detection of a variety of attacks including Denial of Service, CGI/WWW, buffer overflow, windows and UNIX vulnerability, unauthorized access and hacking, ARP detection, IP spoofing and more. It also protects against worms, Trojans, etc.
Sax2 allows us to configure the security policy with fine-grained controls. Real-time alerting and response to alerts is provided by Sax2. It allows for advanced traffic analysis, log generation, and in-depth packet decoding. These can be used to generate traffic usage reports and the statistical traffic analysis tools add to these capabilities.

In this vein, it also provides for monitoring individual conversations and packet streams (or flows). A Name Table provides a list of aliases for addresses, port numbers and protocols on the LAN, and this can be used to set up different names and colors to make it easier for the administrator to narrow in on specific information in the future

3.3 REASONS TO SELECT Sax2.0

Network Based

Sax2 is a network-based IDS. It collects, filters, and analyzes traffic that passes through a specific network location. A single Sax2 monitor, strategically placed at a key network junction, can be used to monitor all incoming and outgoing traffic for the entire site. Sax2 does not use or require installation of client software on each individual, networked computer.

Intrusion Detection and Prevention

Detects variety of complex attacks in the network, including pre-attack detection, password guessing, denial of service attacks (DoS/DDoS), buffer overflow attacks, CGI/WWW attacks, windows vulnerabilities attacks, Unix vulnerabilities attacks, unauthorized access, abuse of network resources, worms, backdoor Trojans, ARP deception, and so on. And then, Sax2 will initiatively stop the dangerous behavior to prevent the whole network.

Traffic Analysis

With its real-time display and statistical traffic analysis of whole network, you may find network resource abuse, worms, denial of service attacks, to lead the network work well.

Logs of Events

Records the actions and sensitive events in whole network, including the WEB browser, Email transmission, FTP transfers and instant message - MSN to help network administrators identify potential threats.

Customize Security Policy

According to the user's own network, IT professional may customize the security policy to improve the accuracy of intrusion detection.

Real-Time Alert and Response

Multiple response modes are available in Sax2 like send console message, logs, e-mail inform, real-time cut off the connection, flexible logs.

Name Table

The name table allows you to make or edit alias for addresses, ports and protocols, you may also specify the text color for a selected item. This useful feature can make packet-related information familiar and intelligible.

Support multi-adapters

If you have more than one adapter installed on the local machine, Sax2 can capture the traffic on all the adapters.

In-depth Packet Decoding

Provides detail packet decoding information.

Conversation & Packet Stream

Monitor all conversations and reconstruct packet stream.

3.4 INSTALLING THE TOOL AND SYSTEM REQUIRMENT

Sax2 is freeware and can be downloaded from various sites offering free downloads. Some well known sites are

http://wareseeker.com
http://www.freedownloadscenter.com/
http://3d2f.com/
http://sax2-intrusion-detection-system-free-.smartcode.com
http://www.ids-sax2.com/

a) After selecting download, new option prompt screen will automatically be open to proceed (if download screen does not appear first attempt, please use other link provided on the same page or different page)
b) Sax2 is 5.52 MB file. You can save this file on the system by clicking SAVE or can directly install by clicking RUN button. (I prefer the SAVE option as you may use it later for installation)
c) By following some simple clicks (mostly NEXT option) Sax2 will be installed on your computer. You can create the desktop icon or can run it from start by selecting *Intrusion Detection System – sax2* option
d) If your computer has more than one adaptor, you may need to select the right adaptor on where Sax2 must perform the Intrusion Detection.

Operating Systems
Win 2000/NT, Windows XP, Win 2003, Windows Vista
Size 5.52 MB
System Requirements
Ax3soft Sax2 can be installed on many Windows operation systems, such as Windows 2000, Windows XP, Windows 2003 and Windows Vista and x64 Edition. Your system's performance and configuration will affect the running status of Ax3soft Sax2. The following minimum requirements are the base line to install and run Ax3soft Sax2ly.

It would be better if your system has a higher configuration, especially in a busy or big network.

a). **Minimum requirements**: P4 1.2G CPU, 512 MB RAM, Internet Explorer 5.5 or higher

b). **Recommended requirements**: P4 3.0G CPU, 1 GB RAM or more, Internet Explorer 6.0 or higher

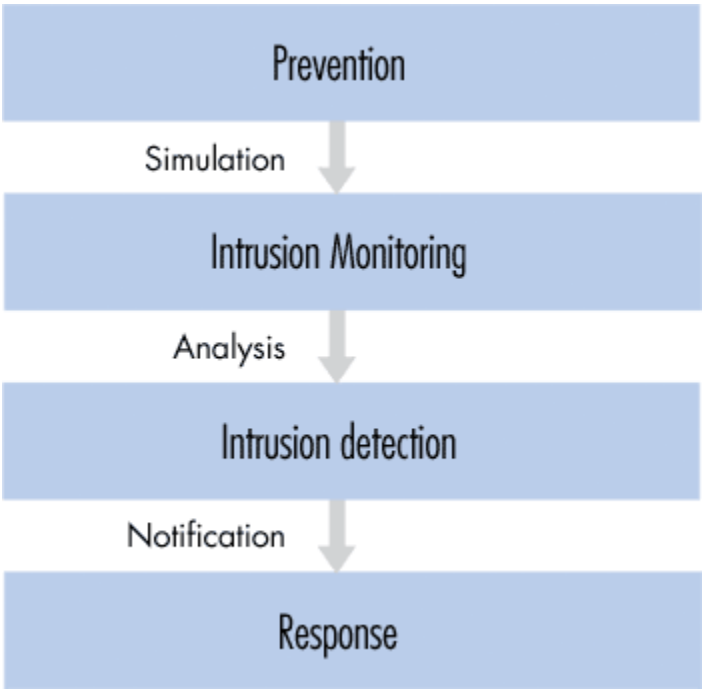
c). **Supported Windows Platforms**: Windows 2000 (SP 4 or later) Windows XP (SP 1 or later) and x64 Edition, Windows Server 2003 (SP 2 or later) and x64 Edition, Windows Vista and x64 Edition
Notes: You are required to have the "Administrator" level privileges on supported operating system in order to load and unload device drivers, or to select a network adapter for using the program to capture packets.

PROJECT EXECUTION

4.1 PART OF THE PROJECT BEING EXECUTED USING SELECTED TOOLS

During the execution of the project using tool Sax2.0, documenting the project and experiencing firsthand the capabilities of Sax 2.0, I will get in depth working of the tool. Create two or more computer network. Attack one computer from the other and will detect the intrusion on the attacked computer using the tool.

Step 1 Create a network of two or more computers.
Step 2 Install Sax2.0 on the computer1. Configuring it and test it to detect the intrusion
Step 3 Make a computer2 ready for attack and generate the attack on Computer1 using the tool
Step4 Detect the Intrusion on Computer1 and perform the various functions offered by the Intrusion Detection System Sax2.0.
Step5 Try to make some changes in the network as well as machines to minimize the effect of Intrusion on a system. Also study various ways to minimize the intrusion on the network and on the machine.



Intrusion detection system activities

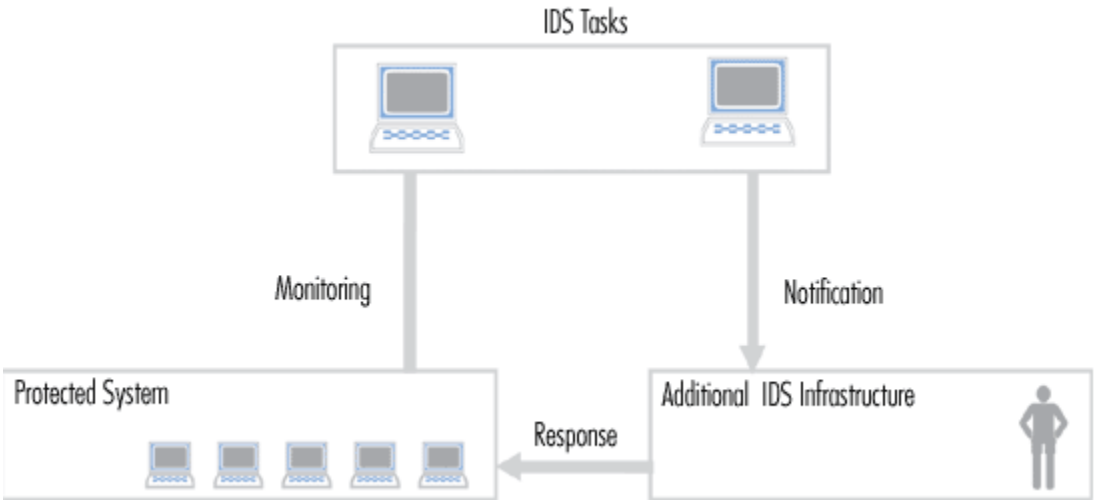
4.2 WHAT HAS BEEN LEARNED FROM THE PROJECT

I have learned about Sax 2.0 and wireshark, what they do and what they are used for. I have gained some experience using the programs and have familiarized with software's.

This will be useful for my practically demonstration and learning the tools on various networks and understand in depth execution of the tools.

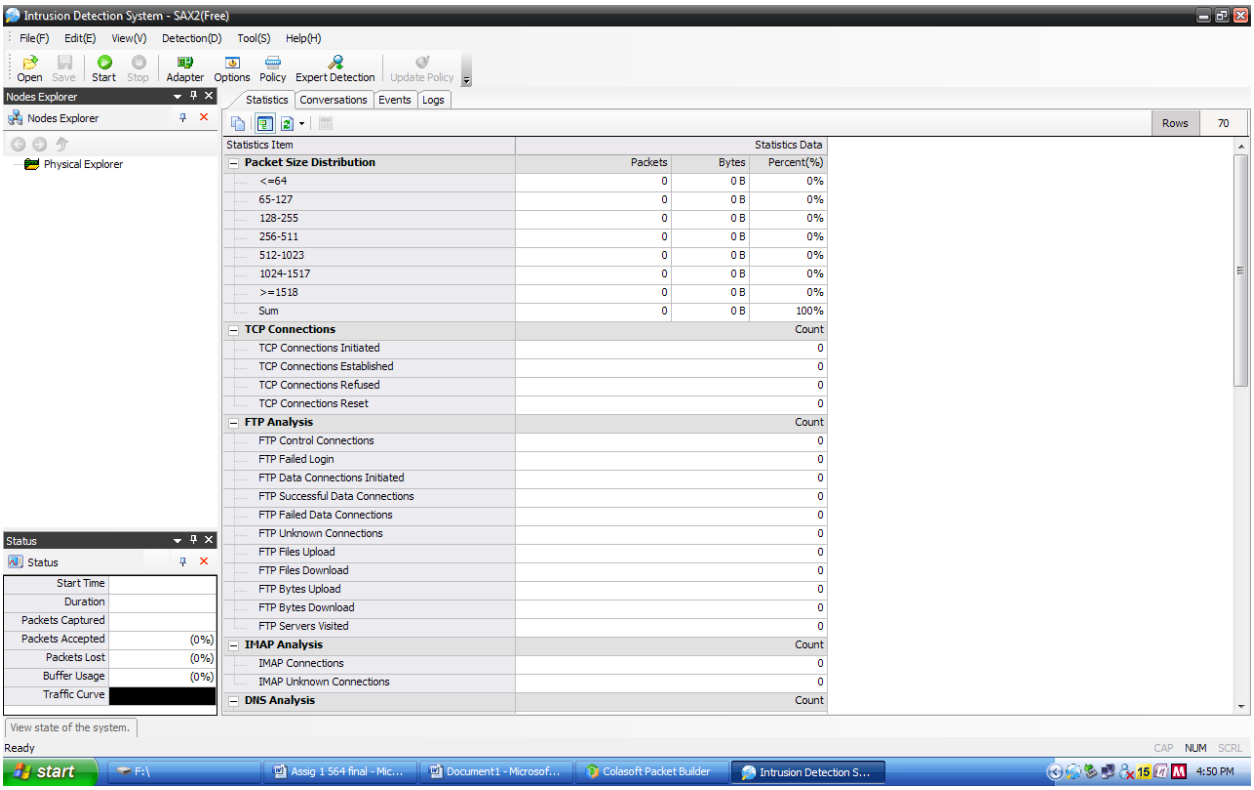
I will focus on some of the pros and cons for using Snort and for using Sax 2.0. While doing research we found many other resources and tools that are in the internet offering intrusion detection and intrusion prevention as I mentioned on this paper above. This project is very informative and helpful for research new tools to use to protect a network or home personal computer from the intrusion.

After successfully executing the project and focusing on the pros and cons in the selected tools and network, I will make a detailed presentation in power point to demonstrate tool working, my project execution, result of the project and ways to eliminate intrusion internally and from outside the system (internal and external intrusion)

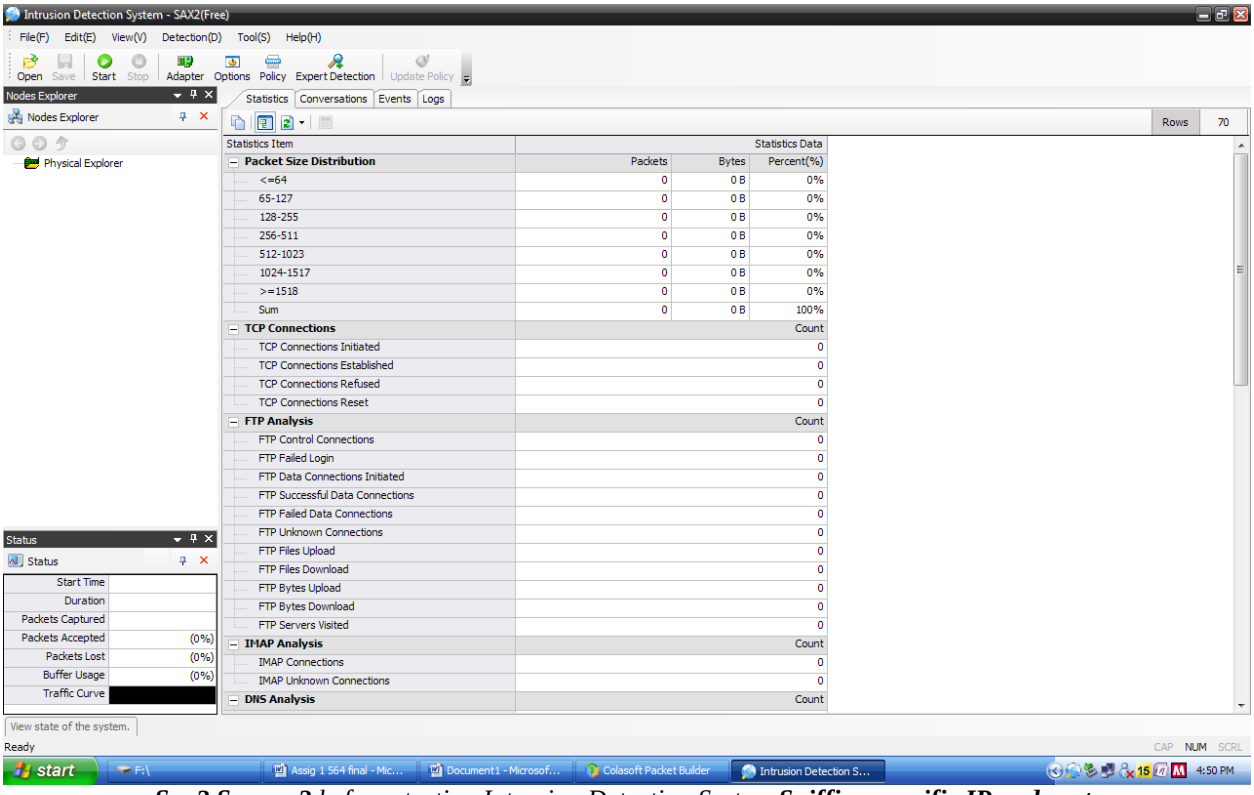


Intrusion detection system infrastructure

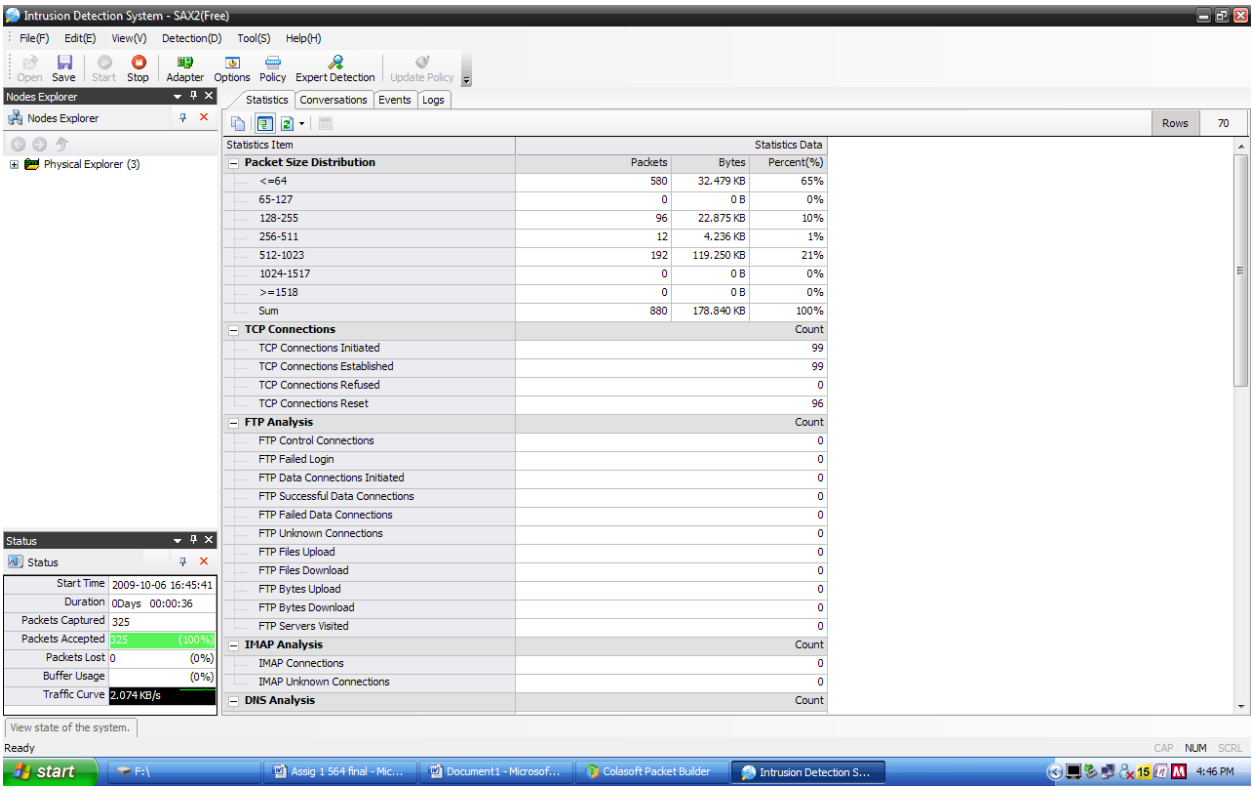
SCREEN SHOOTS FOR INTRUSION DETECTION TOOLS



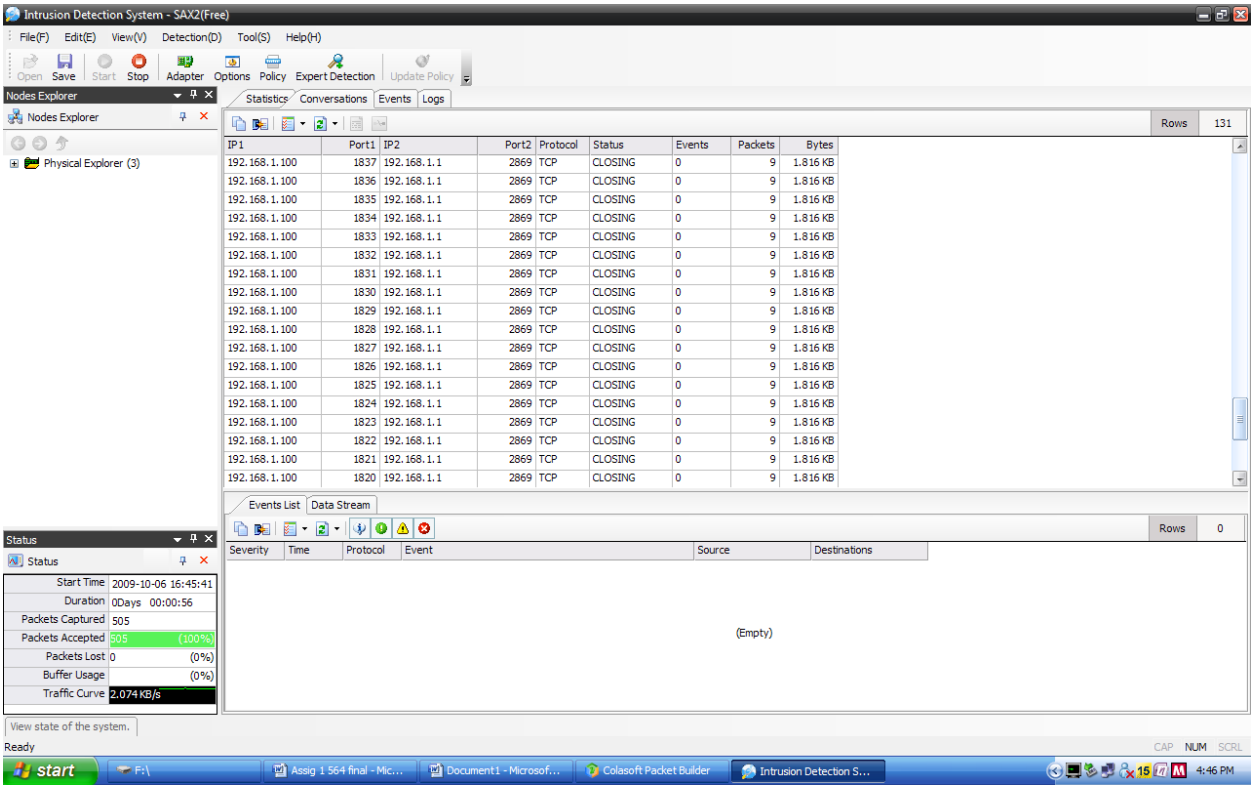
Sax2 Screen 1 *before starting Intrusion Detection System* ***capturing live packets***



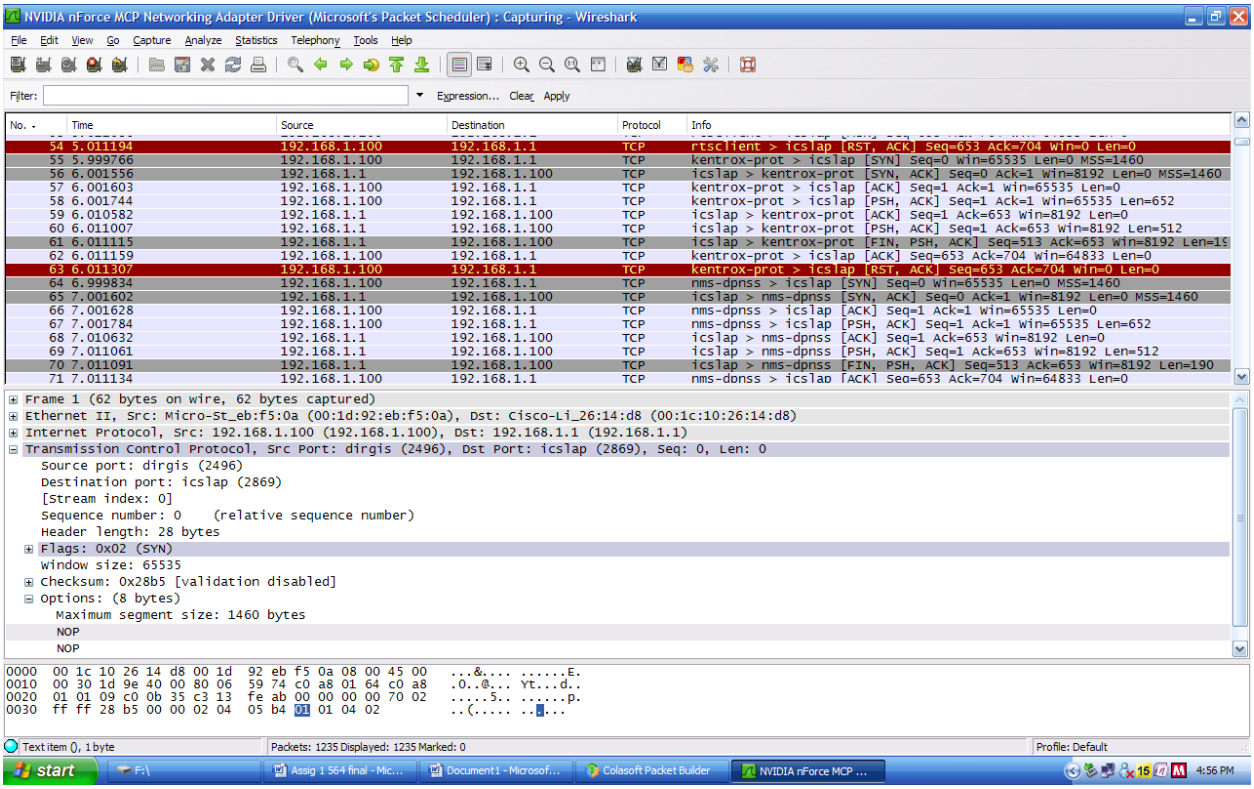
Sax2 Screen 2 *before starting Intrusion Detection System* ***Sniffing specific IP and port***



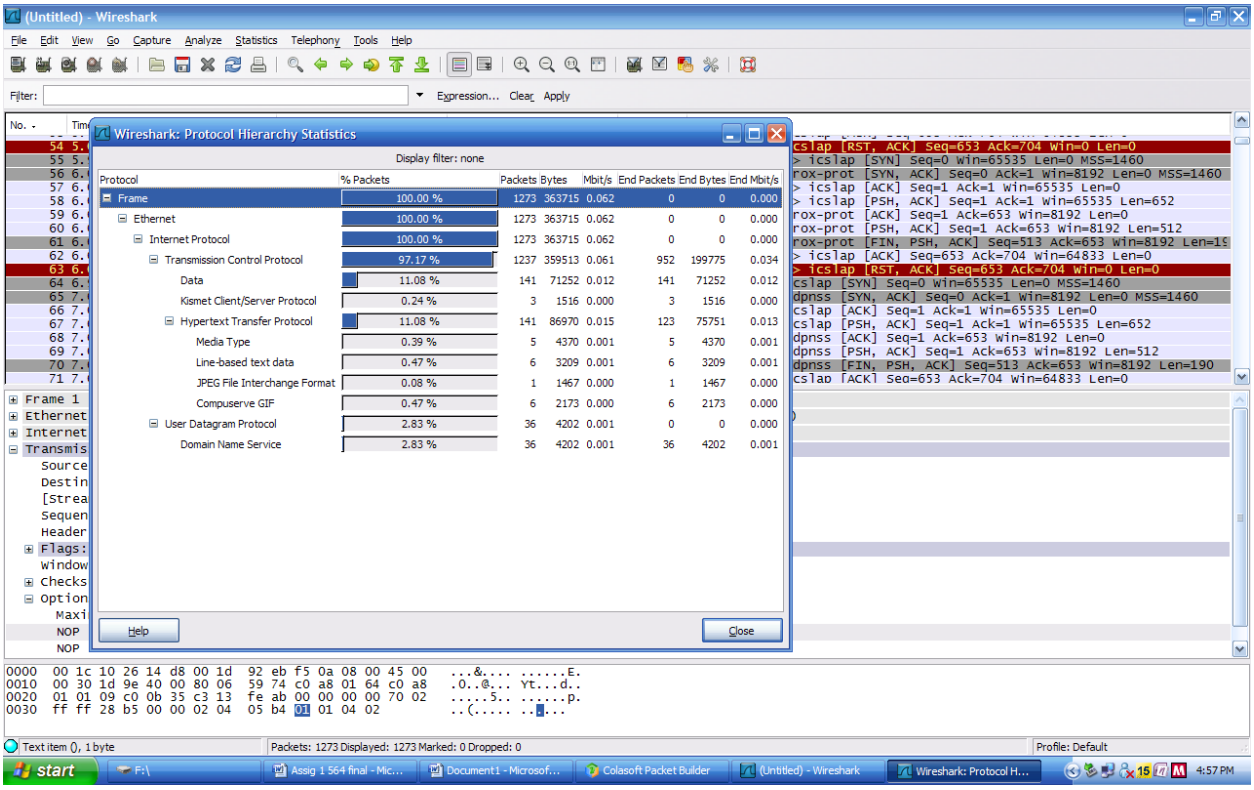
Sax2 Screen 3 *after starting Intrusion Detection System* ***capturing live packets***



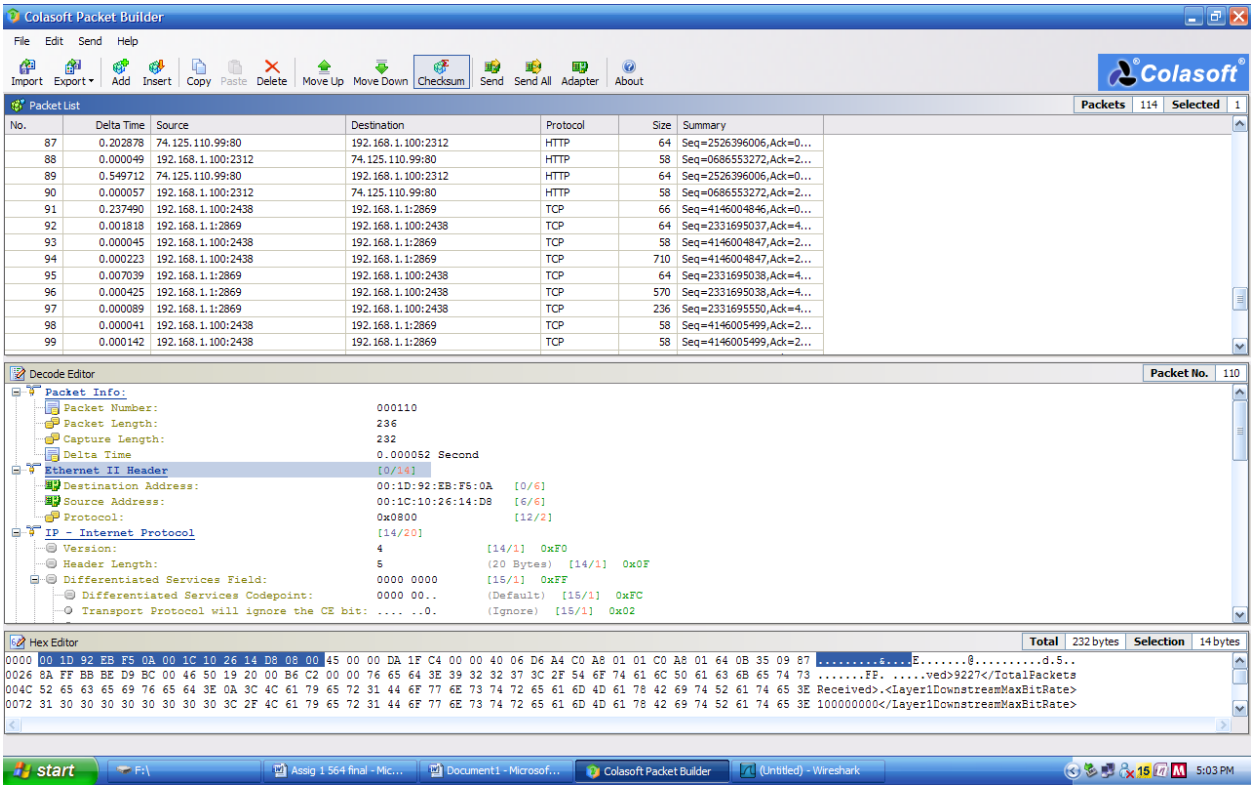
Sax2 Screen 4 *after starting Intrusion Detection System* ***Sniffing specific IP and port***



Wireshark screen 1 *Live capturing of the packets using wireshark on the network. Source IP and Destination IP*



Wireshark screen 2*: wireshark Protocol Hierarchy statistics for above capturing screen.*



Colasoft screen 1 *Live capturing of the packets using* ***colasoft packet builder*** *on the network.*

REFERENCES

[1] **Book** Network Defense and Countermeasures: Principles and Practices, Chuck Easttom. Prentice Hall, 2006. accessed on Sept 26/ 27/ 28/ 29, 2009
[2] Appendix B. SAX 2.0 Features and Properties, O'Reilly.
http://docstore.mik.ua/orelly/xml/jxml/appb_01.htm accessed on Sept 30, 2009
[3] Class notes 0360564 Intrusion detection
http://web2.uwindsor.ca/courses/cs/aggarwal/cs60564/materials.htm accessed on Sept 30, 2009
[4] What is network intrusion system?
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#1.1 accessed on Oct 01, 2009
[5] Architecture
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#2. accessed on Oct 01, 2009
[6] Policy and prevention
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#3. accessed on Oct 02, 2009
[7] IDS and firewalls
http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#7. accessed on Oct 5, 2009
[8] Intrusion detection Systems - Wikipedia
http://en.wikipedia.org/wiki/Intrusion-detection_system accessed on Oct 03, 2009
[9] Intrusion and intrusion detection
John McHugh, Alan Christie, and Julia Allen
Software Engineering Institute, CERT Coordination Center
http://www.cs.virginia.edu/~jones/IDS-research/Papers.html accessed on Oct 05/ 06, 2009

DOWNLOAD

Sax2 Intrusion detection System (freeware) 3.1
http://www.tucows.com/preview/601069 accessed on Oct 02, 2009
WIRESHARK (freeware)
http://www.wireshark.org/download.html accessed on Oct 01, 2009
Colasoft Packet Builder 1.0 (freeware)
http://www.colasoft.com/packet_builder/ accessed on Sept. 25, 2009

----------end of document----------