

Host Based Intrusion Detection System

Technical Details

Introduction

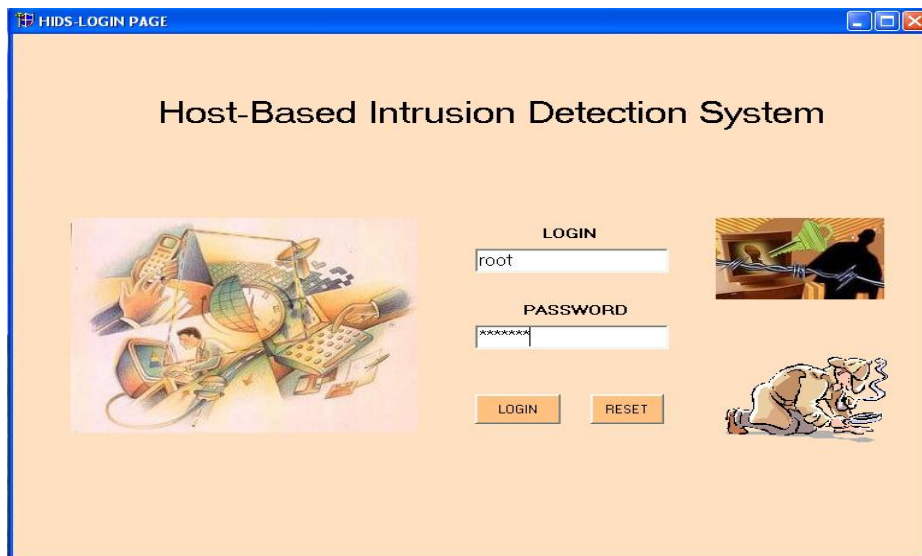
Host Based Intrusion Detection System is software used by the system administrator to detect intrusion and also for the analysis of network based on the packets as well as the users that are currently connected to the machine. It also provides an interface for framing rules and also for statistical and graphical analysis of the available data.

System Requirements

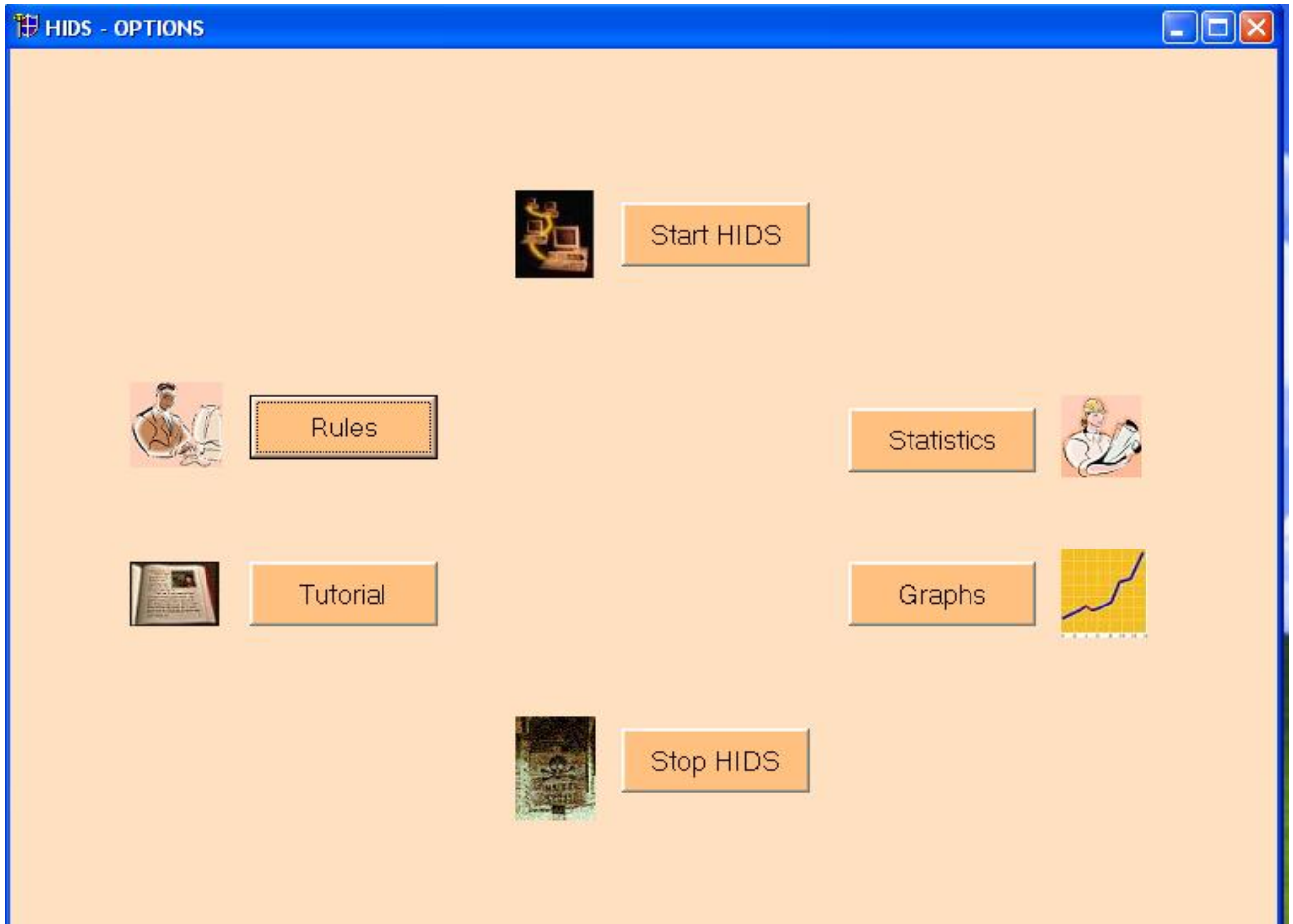
HIDS has been successfully tested and has provided optimum results on MS Windows XP platform with 256 MB RAM , 1.66 G Hz processor . To generate the interface Visual Basic 6.0 has been used and for the capture of packets , generation of user information , database connections Visual C++ 6.0 has been used and for the creation of setup file Visual FoxPro has been used .

Features

The HIDS comes with an interactive interface which is provided with a login screen at the beginning of the executable .The login and password of the HIDS are “root” and “iiit123” .



Error checking with regard to the login and the password of the form have been dealt with and a message box is popped up upon error . Reset has also been provided with . Upon successful entry into the HIDS , we come across a form with various utilities which are present in HIDS which include the Running HIDS, Statistical Analysis , Graphical Analysis , Writing as well as Deleting the rules .



These are the various options which have been provided . Now let us look at each option explicitly . First and foremost Tutorial

Tutorial

The tutorial deals with the basics of the implementation of the rules. The rules can be implemented as follows

DestPort=139 AND PacketSize > 3000

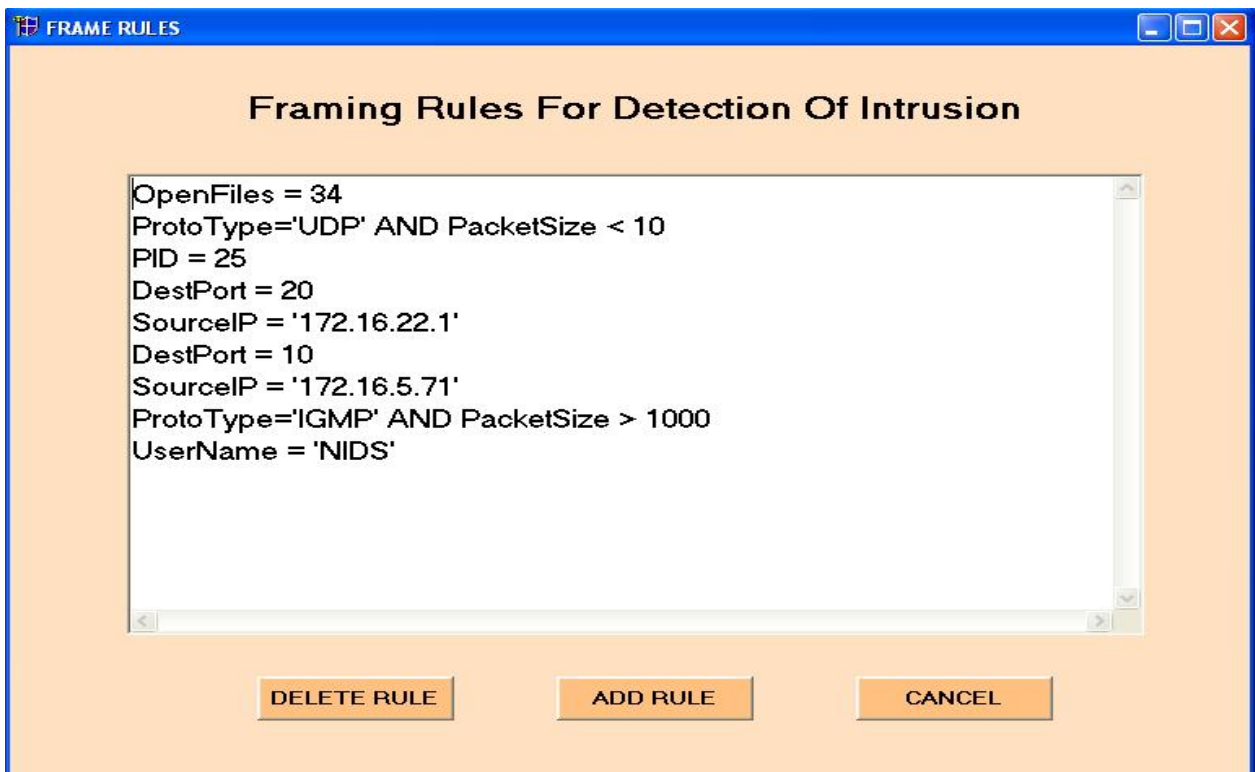
Thus the rules can be any combination of the various attributes which are present in the packet and the network tables

The following is the list of the various attributes.

🔑	PID		
	ProtoType		
	SourceIP	🔑	NID
	DestIP		UserName
	PacketSize		ComputerSrc
	ArrvTime		OpenFiles
	SourcePort		IdleTime
	DestPort		LogTime

Any logical combination of conditions on various attributes present in these tables can be used . These rules are used to check the detection of the intrusion

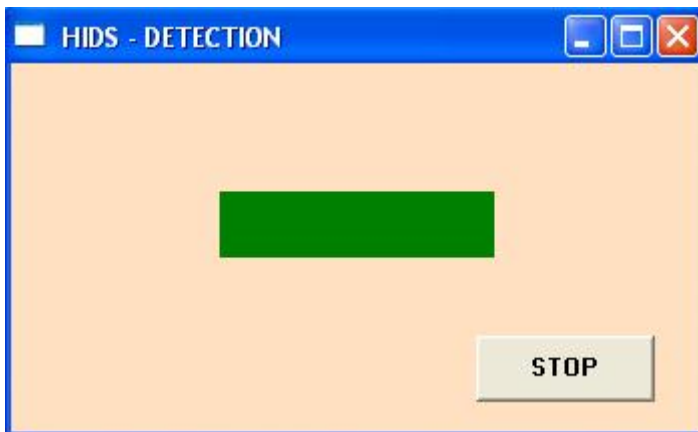
Rules



The above figure shows the rules with the options to delete, add rules . In order to delete rules all that we need to do is to specify the rule no that we want to delete and regarding the addition of the rule , we need to specify the rule in the given text box

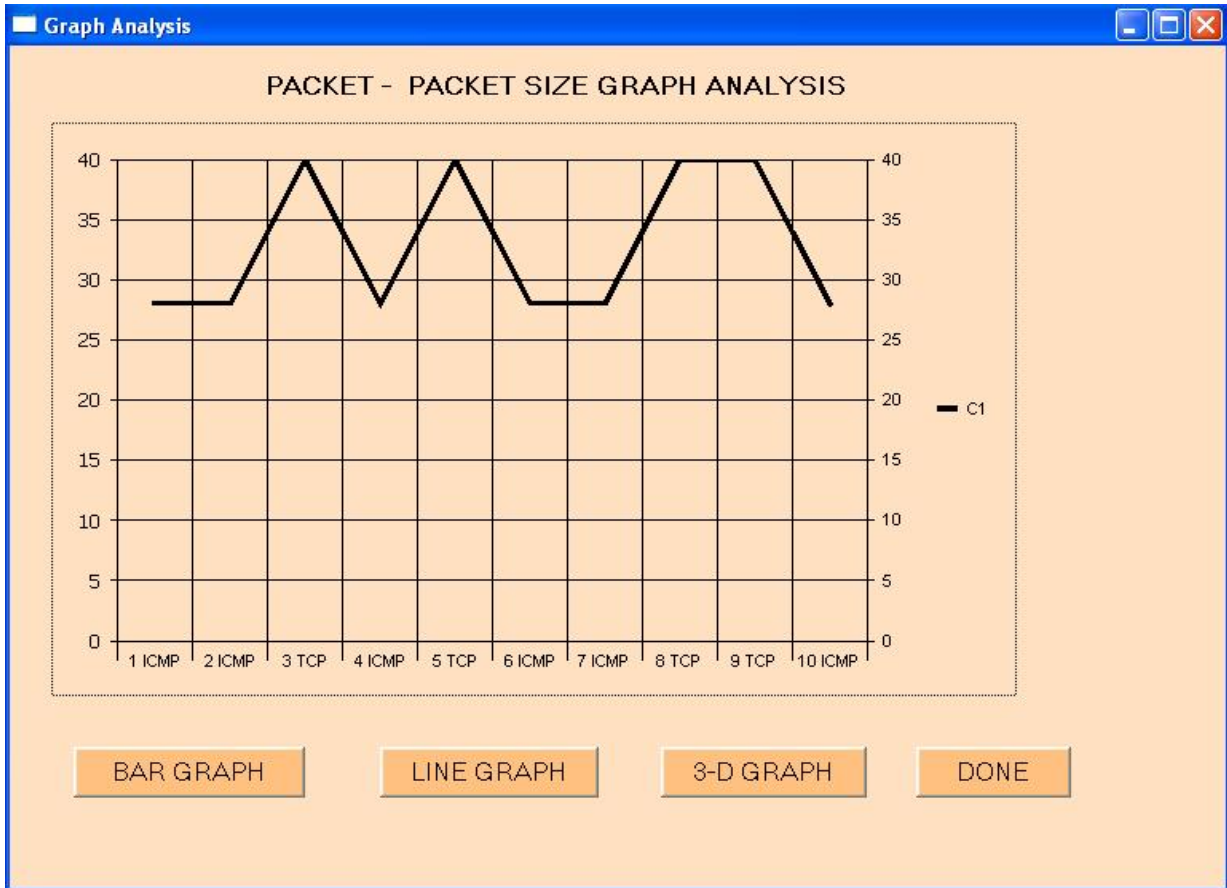
Running HIDS

HIDS can be run by clicking of the Command Button RUN HIDS . This will open a dialog box which has the following color codes. White if the processing is going on , Green if the system is not intruded into , Red if the system has been intruded. Thus when the intrusion is detected a window gets popped which shows the tuple that has violated the rule . Thus the cause for the intrusion can be found out easily .Also a sound will be emitted which will set the sys admin on an alert. The HIDS if not stopped will run for an infinite amount of time . The STOP button can be used to stop the HIDS which will lead us back to the options page



Graph Analysis

There are three different types of graph analysis available ranging from the line graph, bar graph to the 3-D graph on the various packets and their sizes. These can be used by the admin to find out the normal packets that are commonly used and also their sizes. Thus graph analysis proves out to be a good way of finding the basic idea of the network and the packets that are associated with it



Statistics

This form provides us with the various different attributes and the various maxima associated with it like the user that has connected to the machine for the most number of times, the packet with the maximum size so on and so forth

Thus these utilities and features have been provided in the HIDS package

Backend Programming

Backend involves getting the information and updating the database. Packet capture has been done using Windows Sockets. The file that has to be included is winsock2.h and the ws2_32.dll has to be added in the project settings under links. Next the user information is got using the net.exe present in the system 32 folder of Windows. The contents of these are parsed into a file which is read by another program which updates the database based on these connections. For the database connections we have used OLEDB driver and the C:\Program Files\CommonFiles\System\ado\msado15.dll has to be imported. The Source Codes for all these programs has been provided in the folder along with the executables that have been generated. The executables that have been provided are Insert_Packet.exe, Delete_Packet.exe, Insert_Network.exe, Delete_Packet.exe which are self explanatory. Sniffer.exe must be placed in the system 32 folder which is done by the setup file. These applications run independently and these update, delete the database.

Interface Programming

Interface Programming is done using Visual Basic 6.0. The executables are synchronously run so that the updating and deleting from the database are not done simultaneously. These are taken care by the timer control and the Sleep function which are present in the Visual Basic.

The Visual Basic also makes use of the OLEDB for the connection to the database. Other details regarding the use and the various forms that are present has been provided in the Documentation and also the source code which has been commented extensively. Thus these are the various options that have been provided for giving the system administrator friendly interface which is both fast and easy to understand. Tutorial and Documentation have also been provided with.

Improvements

The following are the improvements that can be made

- Change Password option has to be provided in the Login page of the interface
- Deletion of Rules should be made more easier either as a notepad or range of values getting specified instead of a single line number
- For the tuples that are causing violation there should be only a single message box getting displayed
- Tutorial should be more extensive
- For Graph and Statistical Analysis a combo box must be provided for more advanced options

- Error checking and also spelling check should be done while adding a new rule
- Deletion is a bit frequent because of which the time taken for a single cycle is around 30 secs which can be removed by avoiding the deletion which means that the synchronization is not required and so the HIDS time for detection would increase drastically
- However the deletion should take place when the CPU usage is less
- Oracle can be used for decreasing the database access time or an option can be given by even developing an Oracle Version of the code
- The most important improvement that can be done is to develop a NIDS which can deal with the packet and network statistics over a network from a single host machine

Credits

This software has been done as our semester project under **Prof Ch.Venkaiah , IIIT**. The members of this project are K.Sumanth ,C. NavyaLatha , Gaurav Kumar Somani, Venkat Kumar.G . We would also like to take this opportunity to thank our mentors Aizaz and Hemanth for the wonderful support that they have given us . It has been a great experience doing this project during which we learnt lots of interesting things on networking

Contact

venkaiah@iiit.net

sumanth@students.iiit.net

navya@students.iiit.net

gaurav_k@students.iiit.net

venkat_kumar@students.iiit.net