A Simplified Approach to Identify Intrusion in Network with Anti Attacking Using .net Tool.

[1]Sumit A. Khandelwal, [2]Shoba. A. Ade, [3]Amol A. Bhosle and [4]Radha S. Shirbhate

***Abstract*—While advances in computer and communications technology have made the network ubiquitous, they have also rendered networked systems vulnerable to malicious attacks orchestrated from a distance. These attacks, usually called cracker attacks or intrusions, start with crackers infiltrating a network through a vulnerable host and then going on to launch further attacks. A problem with most of the security systems like antivirus and firewalls is that they provide security at application layer only leaving the system open to various modern attacks. One of the solutions to this problem is to develop an Intrusion Detection System that provides security at all the three layers i.e. application, transport and IP layer. An Intrusion detection system (IDS) is software designed to detect unwanted attempts at accessing, manipulating, or disabling of computer systems, mainly through a network, such as the Internet. In this project, we have implemented an Intrusion detection system that not only detects intrusions at various layers, but is also capable to counter attack on the intruder's machine such as send a warning message or even shutdown it. In our paper we can introduce intrusion detection system with Anti Attacking using concept Microsoft Visual Basic 2005 (.net), .net provides popular and low cost for technical education modeling technique and secure techniques for in network.**

***Index Terms*—ACL, API, IDS, Anti-attacking.**

I. INTRODUCTION

Intrusion detection (ID) is a rapidly evolving and changing technology. Intrusion detection systems first appeared in the early 1980s [1]. While statistics on the growth of attacks provide a more solid basis for justifying the need for intrusion detection (ID), case histories can often be more persuasive. Over the past few years, the growing number of computer security incidents on the Internet has reflected the growth of the Internet itself. Because most deployed computer systems are vulnerable to attack, intrusion detection (ID) is a rapidly developing field. Intrusion detection is an important technology business sector as well as an active area of research. In the 1980s, intruders were the system experts. They had a high level of expertise and personally constructed methods for breaking into systems. Use of automated tools and exploit scripts was the exception rather than the rule. Today, absolutely anyone can attack a network due to the widespread and easy availability of intrusion tools and exploit scripts that duplicate known methods of attack Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource." An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Typically, we say that an intrusion has taken place when an attack is considered successful from the victim's perspective, i.e., the victim has experienced some loss or consequence.

A successful attack is enabled by the presence of vulnerability in the victim's system that is exploited by an intruder with an objective. We use the term intrusion to mean a successful attack. An attack is unsuccessful from the perspective of the intruder if none of their objectives are fulfilled; whereas, a victim perceives an attack as unsuccessful if there are no consequences that result from the attack. Unsuccessful attacks from the perspective of an intruder may still have one or more consequences for a victim. A new technique of proactively detecting intrusion is to lure attacker to attack and record their signature. Then by means of intrusion prevention these attackers can be dealt carefully. This technique is called as deception. There are two types of intrusion detection schemes: anomaly-based and rule-based. Anomaly-based IDS (Intrusion Detection System) model watches for activities that are different from a user's or a system's accepted normal behavior. A rule-based (or signature-based) IDS model, on the other hand, watches for activity that is similar to known patterns of attacks.

II. LITERATURE REVIEW

A. Security Concerns

Despite nearly universal efforts to protect corporate networks, today's distributed organizations are still susceptible to a multitude of attacks. IT executives are challenged to extend security beyond the corporate backbone to protect a variety of potential vulnerabilities, including Internet connections, communication channels between remote and corporate offices and links between trusted business partners. Unfortunately, the preventive measures employed to secure corporate resources and internal traffic doesn't provide the breadth or depth of analysis needed to identify attempted attacks or uncover potential threats across the organization.

B. Network Security Management

Network Security Management is a process in which one establishes and maintains policies, procedures, and practices required for protecting networked information system assets. Security is the process of staying informed. The goals of security include Confidentiality (ensuring only authorized users can read or copy a given file or object), Control (only authorized users can decide when to allow access to

Manuscript received December 13, 2010; revised March 13, 2011.

information), Integrity (only authorized users can alter or delete a given file or object), Authenticity (correctness of attribution or description), Availability (no unauthorized user can deny authorized users timely access to files or other system resources), and Utility (fitness for a specified purpose).

III. INRUSION DETECTION SYSTEM (IDS)

A. Intrusion detection

Intrusion detection technology is technology designed to monitor computer activities for the purpose of finding security violations [1]. An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of 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 [2]. A successful attack subverts the execution of a vulnerable process in a manner undetectable to an execution monitor. We consider two threat models meeting this definition. Bypass attacks exploit design deficiencies of a detection system to avoid the execution monitor and generate arbitrary unmonitored system calls [6]. The system calls executed by the attack may not be allowed by the execution monitor; unfortunately, the monitor never intercepts the calls of a bypass attack. Transformational attacks, such as a mimicry attack [3, 4, 5], alter a detected attack so that it goes undetected by the model-based detection system yet carries the same malicious intent. A transformational attack is allowed by the program model. 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. An Intrusion detection system (IDS) is software or hardware designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by hackers, malware 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).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 hat 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 IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. Current exploits against processes executing on Windows work differently. All operating system kernel traps are intended to be executed only by Windows subsystem shared libraries and not directly by applications. Windows exploits largely obey this programming practice, so library call enforcement would detect most current Windows attacks. This exploit design is largely an artifact arising from the obfuscated set of Windows kernel traps. The kernel trap interface is not widely published and may change between operating system releases. Yet, details of the Windows trap interface, called the "Native API", are available to interested attackers [7].These attackers can convert an attack that calls subsystem library functions into an attack that directly invokes Windows kernel traps. Although library call verification may detect today's attacks, with little effort attackers can alter their Windows exploits to bypass the library call interface. Recent intrusion detection systems monitor a combination of kernel traps and function call return addresses stored on the call stack [3, 8, 9]. It is important to understand the utility of function call monitoring given the knowledge that the function call interface is circumvent able [3]. In many simple IDS implementations all the components are combined in a single device or application.

B. Anti-attacking

In many organizations there are network uses in which many client systems are connected to each other through a channel. This is essential to communicate client with each other or Administrator. So in organization LAN or WAN network is established as there working need .So there can miss use of system by the client such that he can operate illegal operation or the client can be idle on his system. This can be dangerous to the organization so we have developed the LAN monitoring system application in which the Administrator monitor several clients which are connected in network and there can be several administrators. If a client in LAN is detected as an intruder, the administrator can continuously monitor the client system by watching running processes and hardware configuration and can take appropriate action .If he finds anything going wrong on particular client he can send appropriate message to that client also the administrator can shut down the particular client's system if it requires.

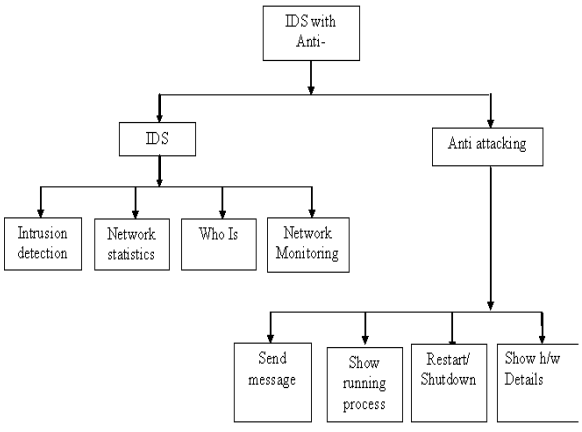

Fig.1. Project Data Flow Diagram

IV. PROBLEM DEFINITION

There are number of challenges to be faced for providing network security.[2] Most of the security systems aims at providing security at only application layer, but as technology is advancing day by day, hackers and intruders are developing techniques which attack on transport and IP layer also thus it is essential to develop an security system that provides multilayer security. Many IDS system is running and used by the network administrators but the major problem with all these are that they are capturing and generating reports as per client requirements [3]. Proposed systems is mainly aimed at getting intruder's IP address and then track all the activities done by the intruder system to generate its activity log and to do cross attack on the intruder system.

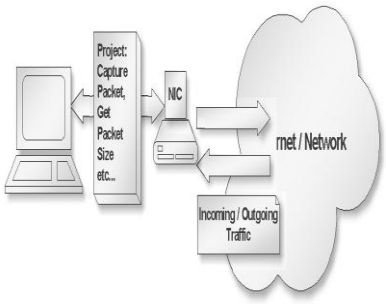

Fig 2. Basic idea of the project

Figure 2. Show the system is connected to the network through LAN card and we are running the application on system which will keep track of the incoming and outgoing packets information. Proposed system will create object of LAN card driver where data reached first. Whenever data come to system it will first get to LAN card object. Without filtering we can get any type of data from here for that we need to control this object. O. S. provides many API to get the driver object and its information. When data get transferred it will fill the LAN card structure.

A. Remote Controlling the Client

In our project, the Client PC will be controlled using another PC. Two PC's will be connected in LAN with each other in network. The Server will connect to the Client, which is on another PC via the socket through the TCP/IP protocols. After both the PC's are connected using the Winsock control, then comes the part of controlling the client PC. It may be controlling the PC, sending a message to client, restarting, shutdown ,view running process ,view hardware details, etc.

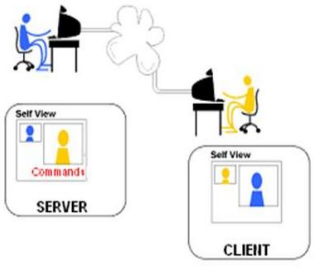

Fig 3. Remote Controlling the Client

V. IMPLEMENTATION

In our project we developed two main modules.

1. Intrusion Detection

This is the main module for intrusion detection in which we are having following four sub-modules:

A. Intrusion Detector

In this module we are starting the defense for our system. It will show all the current running process along with incoming, outgoing, blocked packets. With this module the administrator can allow or deny any process to start its execution. This module define rules i.e. ACLs for intrusion detection. After detecting an intrusion, it displays a warning message, containing details of the intrusion along with the port on which it is trying to access.

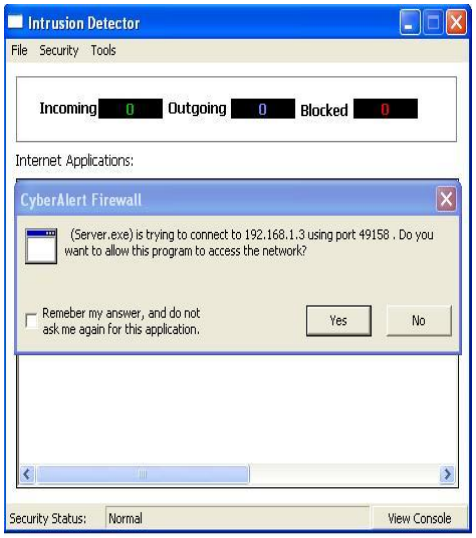

Fig 4. Start Form for intrusion detector

B. Network Statistics

In this module we are fetching the network statistics, all the details about the current ports and also the process which are running on that port. This is the module in which all the detail information about every individual connection can be seen

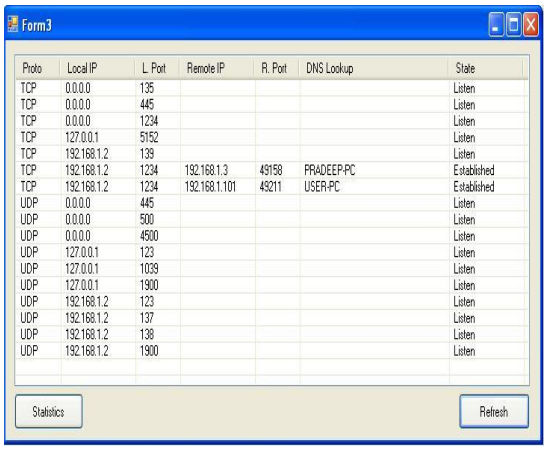

Fig 5.Start Form for network statistics

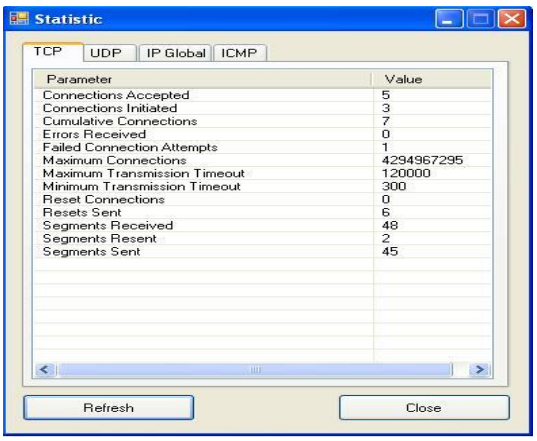

Fig 6. Second Form of network statistics

C. Who Is?

In this module we can get the following information:

- Fetches IP address if DNS name entered or vice versa a WHOIS server.
- Traces the complete route from client to server.
- Displays complete information about the entered IP/DNS.

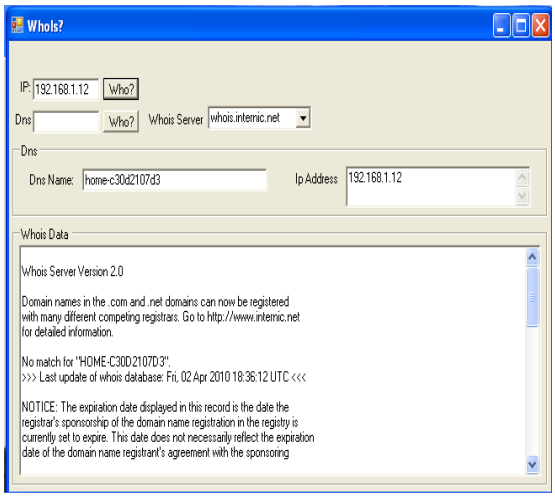

Fig 7. Start Form for who is

D. Network Monitor:

In this module we are scanning the complete network to get all the available nodes in our network along with their Status, DNS name and IP Address.

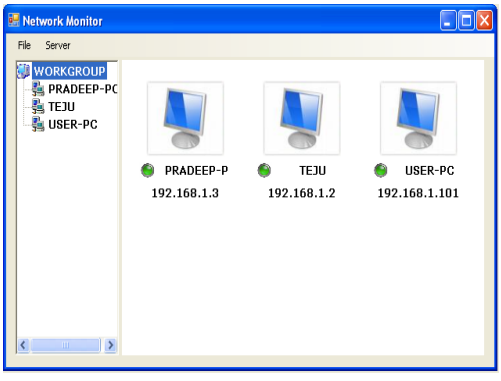

Fig 8. Start Form for Network

2. Anti-Attacking:

This module is shows the lists of client are connected with server in network. Once we establish a connection in network the server computer can send message to client computer in network. Anti-Attacking module which we are having following four functions are perform operation with client computer on request of server computer.

- Send Message
- See Running Process
- Restart/Shutdown client
- See Hardware Details

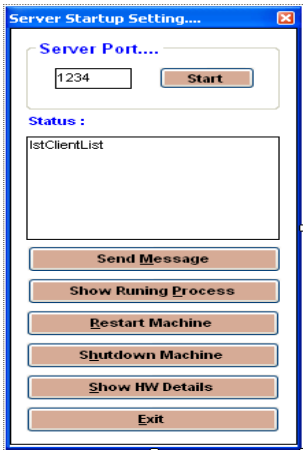

Fig 9. Main interface for anti-attacking

VI. APPLICATION

- This application can be used in any of the organization, colleges, offices etc.
- This can be used to not only for monitoring but also for controlling any number of PC's connected in LAN.
- This application gives the intimation before the system is shutdown or restarted and even replies to the administration.
- It is very helpful in office, where we can control the PC's, which are unnecessarily kept ON by the users.
- It is used in Mobile to mobile control, PC to mobile device control, Traffic light control, and Railway traffic control.
- It is used in Collage Net & Practical Labs, Cyber Cafes.

VII. CONCLUSION

Intrusion detection can be an extremely valuable tool when implemented correctly. Understanding the practical limitations as well as the capabilities of the technology will enable you to achieve the best results and has proved to be the optimum network security system, an intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. In this project, we can detect intrusions using a set of rules defined for intrusion; we can also control execution of various running processes on server as well as client machine. After detecting an intrusion, we can also counter attack on the intruder's machine. Thus this system proves to provide security at

application, transport and network layer efficiently.

Future Scope-

The work presented in this paper is based on the fundamental assumption that to detect intrusion in network and provide a security using anti attacking. One possible probability is that Automatic updating of ACL's defined for intrusion and Provision for desktop sharing and hardware control of intruder's machine. Another possible probability Provision for automatic anti-attacking on intruder should be able to sniff data packet and also capable of accessing internal headers.

ACKNOWLEDGMENT

Our thanks to International Journal of Computer and Electrical Engineering (IJCEE) for allowing us to publish a paper.

REFERENCES

[1] Defending Yourself: The Role of Intrusion Detection Systems *John McHugh, Alan Christie, and Julia Allen, Software Engineering Institute, CERT Coordination Center.*

[2] Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology "*Karen Scarfone andPeter Mell"*

[3] C. Kruegel, E. Kirda, D. Mutz, W. Robertson, and G. Vigna. Automating mimicry attacks using static binary analysis. In *14th USENIX Security Symposium*, Baltimore, Maryland, Aug. 2005.

[4] K. M. Tan, K. S. Killourhy, and R. A. Maxion. Undermining an anomaly-based intrusion detection system using common exploits. In *Recent Advances in Intrusion Detection (RAID) 2002, LNCS #2516*, pages 54–73, Zurich, Switzerland, October 2002. Springer-Verlag.

[5] D. Wagner and P. Soto. Mimicry attacks on host based intrusion detection systems. In *9th ACMConference on Computer and Communications Security (CCS)*, Washington, DC, Nov. 2002.

[6] Anonymous, J. Butler, and Anonymous. Bypassing 3rd party windows buffer overflow protection.*Phrack*, 11(62), July 2004.

[7] M. E. Russinovich and D. A. Solomon. *Microsoft Windows Internals*. Microsoft Press, 4th edition,Dec. 2004.

[8] J. T. Giffin, S. Jha, and B. P. Miller. Efficient context-sensitive intrusion detection. In *11th Networkand Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Feb. 2004.

[9] H. H. Feng, O. M. Kolesnikov, P. Fogla, W. Lee, and W. Gong. Anomaly detection using call stack information. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003.

[10] Behrouz A. Forouzan (2003). TCP/IP Protocol Suite, 2nd, McGraw-Hill. ISBN 0-07 246060.

[11] British Broadcasting Corporation (2004) Research on audience characteristics.http://www.bbc.co.uk/commissioning/market research/audiencegroup2.shtm

[12] By Rod Stephens: "Visual Basic 2005 Programmer's Reference" Publisher: O'Reilly Media; 1 edition (April 25, 2005).

[13] Steven Holzner Black Book for "Microsoft Visual Studio Vb.net"

Sumit A. Khandelwal received his BE degree in Computer Science from Amravati University / India. He is currently an Instructor at the Department of Computer Science and Engineering at JDIET, Yavatmal (India). Since 2009, he is working towards his Master in Computer Science and Engineering from Amravati University. He completed Sun Certification i.e. SCJP and Microsoft certification i.e. MCP, MCTS. He also published various papers in International Journal and Conference also. He is member of IACSIT (Singapore), IAENG (Hong Kong).His research is focused on Image Processing, neural networks and MANET.

Shoba A. Ade received his BE degree in Computer Science from Amravati University /Amravati, he pursuing Master Degree in Computer Science and from Amravati University; she is currently an Instructor at the Department of Computer Science and Engineering at JDIET, Yavatmal (India) since 2004. Her research is focused on Vehicular Ad-hoc network and Network Security.

Amol A. Bosle received his BE degree in Computer Science and Engineering from Amravati University /India, his Master in Business Administration (MBA) Degree in Human Resource from Amravati University /India. His research focus area is Wi-Max Technology and ANN. He is member of IACSIT (Singapore)

Radha S. Shirbate received his BE degree in Computer Science and Engineering from Amravati University /India, his Master in Business Administration (MBA) Degree in Information Technology from Amravati University /India. She also published various papers in International Journal. His research is focused on Network Security.