International Journal of Advanced Research and Review

www.ijarr.in

COMPREHENSIVE STUDY &OVERVIEW OF NETWORK SECURITY

Pravin Wararkar[1], Dr. H K Dahule[2], Lokesh Chawle[3], Sagar Soitkar[3], Ashish Charbe[4], and Jagdish Chakole[5]

[1]Department of Electronics & Telecommunication Engineering, SVKM's Narsee Monjee Institute of Management Studies, (Deemed-to-be-University), Mukesh Patel School of Technology Management & Engineering Shirpur, India, Email: pwararkar@gmail.com
[2] Department of Physics, Shri Shivaji Education Society Amravati's , (Nagpur University), Shivaji Science College, , Congress Nagar, Nagpur, India, Email: hkdahule@yahoo.co.in
[3] Department of Electronics Engineering, Rajiv Gandhi College of Engineering & Research (Nagpur University) Nagpur, India Email: lokesh.chawle14@gmail.com, sagar.soitkar@gmail.com
[4] Department of Electronics & Telecommunication Engineering (Assistant Professor) Rajiv Gandhi College of Engineering & Research (Nagpur University) Nagpur, India, Email: ashishcharbe@gmail.com
[5] Department of Computer Technology, Rajiv Gandhi College of Engineering & Research, (Nagpur University) Nagpur, Indiam Email: jagdishchakole@gmail.com

ABSTRACT

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.Network security starts from authenticating any user. Once authenticated, firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Keywords: Network Security, IPS

Introduction

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired", an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them.Some history of networking is included, as well as an introduction to TCP/IP and internetworking. We go on to consider risk management, network threats, firewalls, and more special-purpose secure networking devices.

This is not intended to be a ``frequently asked questions" reference, nor is it a ``hands-on" document describing how to accomplish specific functionality.

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets.

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them. Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together.
An easy way to look at this is to compare this model with something we use daily: the telephone. In order for you and I to talk when we're out of earshot, we need a device like a telephone. (In the ISO/OSI model, this is at the application layer.) The telephones, of course, are useless unless they have the ability to translate the sound into electronic pulses that can be transferred over wire and back again. (These functions are provided in layers below the application layer.) Finally, we get down to the physical connection: both must be plugged into an outlet that is connected to a switch that's part of the telephone system's network of switches.
If I place a call to you, I pick up the receiver, and dial your number. This number specifies which central office to which to send my request, and then which phone from that central office to ring. Once you answer the phone, we begin talking, and our session has begun. Conceptually, computer networks function exactly the same way.

Fig 1:
The ISO/OSI Reference Model

Intrusion Detection System

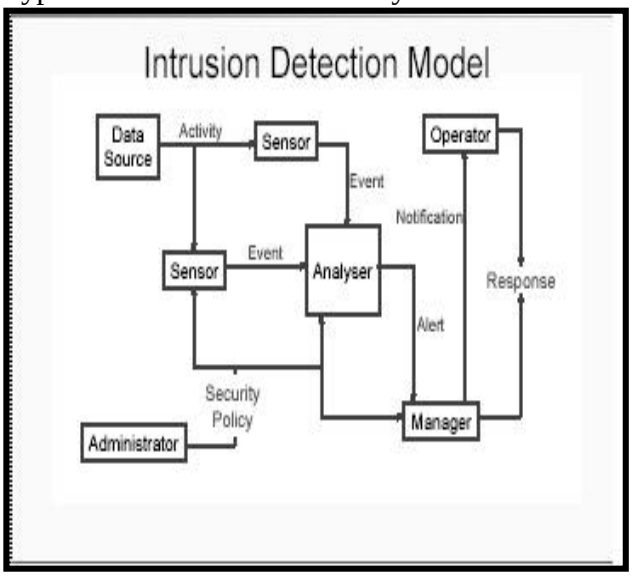
There are two types of IDS. One is network based and real time, while the other is host-based and examines log file data. Network based systems examine all traffic on a system, while host-based systems examine traffic only on that specific system. This is primarily devoted to network intrusion detection system (NIDS).

An intrusion is somebody ("hacker" or "cracker") attempting to break into or misuse your system. The word "misuse" is broad, and can reflect something severe as stealing confidential data to something minor such as misusing your email system for Spam (though for many of us, that is a major issue!).An "Intrusion Detection System (IDS)" is a system for detecting such intrusions.

There are two words to describe the intruder: hacker and cracker. A hacker is a generic term for a person who likes getting into things. The benign hacker is the person who likes to get into his/her own computer and understand how it works. The malicious hacker is the person who

likes getting into other people's systems. The benign hackers wish that the media would stop bad-mouthing all hackers and use the term 'cracker' instead. Unfortunately, this is not likely to happen. In any event, the word used is 'intruder', to generically denote anybody trying to get into your systems.

Types of intrusion detection system There are two types of intrusion detection systems that employ one or both of the intrusion detection methods outlined above. Host-based systems base their decisions on information obtained from a single host (usually audit trails), while network-based intrusion detection systems obtain data by monitoring the traffic in the network to which the hosts are connected.



1. Host-based intrusion detection

A generic intrusion detection model proposed by Denning (1987) is a rule-based pattern matching system in which the intrusion detection tasks are conducted by checking the similarity between the current audit record and the corresponding profiles. If the current audit record deviates from the normal patterns, it will be considered an anomaly. Several IDS's were developed using profile and rule based approaches to identify intrusive activity (Lunt et al., 1988).

2. Network-based intrusion detection

With the proliferation of computer networks, more and more individual hosts are connected into local area networks and/or wide area networks. However, the hosts, as well as the networks, are exposed to intrusions due to the vulnerabilities of network devices and network protocols. The TCP/IP protocol can be also exploited by network intrusions such as IP spoofing, port scanning, and so on. Therefore, network-based intrusion detection has become important and is designed to protect a computer network as well asall of its hosts. The installation of a network-based intrusion detection system can also decrease the burden of the intrusion detection task on every individual host.

Intruders can be classified into two categories.

Outsiders

Intruders from outside your network, and who may attack you external presence (deface web servers, forward spam through e-mail servers, etc.).

Insiders

Intruders legitimately use your internal network. These include users who misuse privileges

The above diagram shows the model of IDS system and our NIDS system works in between the analyzer and sensor.

Fig 2: Intrusion Detection System

Analysis

1. Goals

Main aim of IDS is to protect system from various intrusion attacks. IDS can timely detect when an attacker has penetrated a system by exploiting some vulnerability. Furthermore it can serve an important function in system protection, by bringing the fact that the system has been attacked to the attention of the administrator who can take immediate actions to prevent attacks and recover any damage that results.

- Detect attacks as they happen
- Real-time monitoring of networks
- Provide information about attacks that have succeeded

2. Problem analysis:

Analysis is the most complex element, and can use protocol analysis as well as anomaly detection, graph analysis, etc Common analysis techniques Attempt pattern-matching against certain known attack types. For instance, Substring matching.

The primary ways an intruder can get into a system:

Physical Intrusion:

If intruders have physical access to a machine (i.e. they can use the keyboard or take apart the system), they will be able to get in.

System Intrusion:

This type of hacking assumes the intruder already has a low-privilege user account on the system. If the system doesn't have the latest security patches, there is a good chance the intruder will be able to use a known exploit in order to gain additional administrative privileges.

Remote Intrusion:

This type of hacking involves a intruder who attempts to penetrate a system remotely across the network.

3. Requirement analysis:

3.1 Software and hardware requirements:

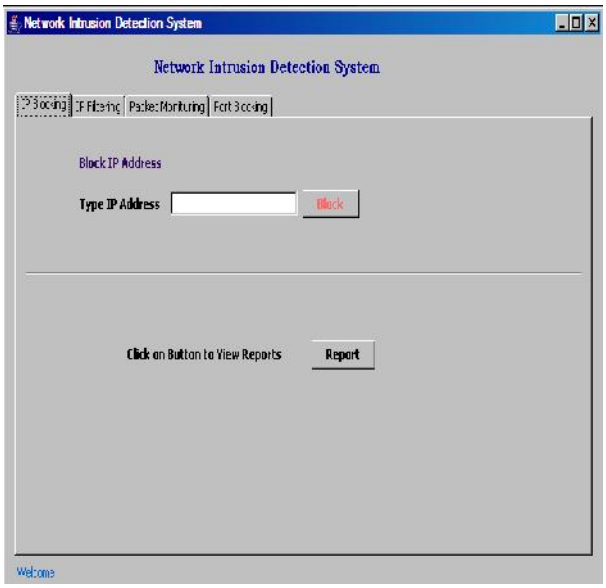
* Operating systems: Windows / Linux
* Language: Java
* Processor: Pentium-II with minimum 10 GB of hard disk.
* Ram: 128MB

MODULES OF NIDS

1. IP Blocking
2. IP Filtering or IP Sniffer
3. Packet Monitoring
4. Port Blocking

1. IP BLOCKING:

IP Blocking is separated into two parts: first one for blocking an IP address and second for viewing the report as shown in the figure.



- **Blocking of an IP address:**

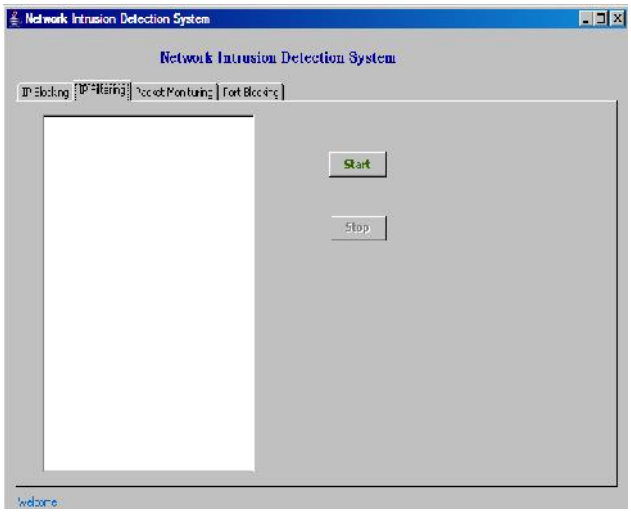
In this block there is a text box for entering the IP address from which we have threat and a button block for blocking that IP address.

- **View the report:**

In this part we can view the list of blocked IP address named as Blacklist which is maintained in a text file with the date and time of blocking and it also display the purpose as shown in figure

2. IP FILTERING or IP SNIFFER:

IP filtering consists of a text area and two buttons (Start and Stop) in which when one is ON the other will be OFF. The text area is for IP addresses for blocked IP addresses from which we allow the packet The buttons are used to start and stop the thread



3. PACKET MONITORING:

Packet monitoring consists a text area, list box, a combo box and a button named start logging. Each has its own use as given below:

- **Combo box:**

A combo box gives the option of a multiple selection in which we can select one or more options. In Packet monitoring, this box is used for selecting a Network Interface Card.

- **Button:**

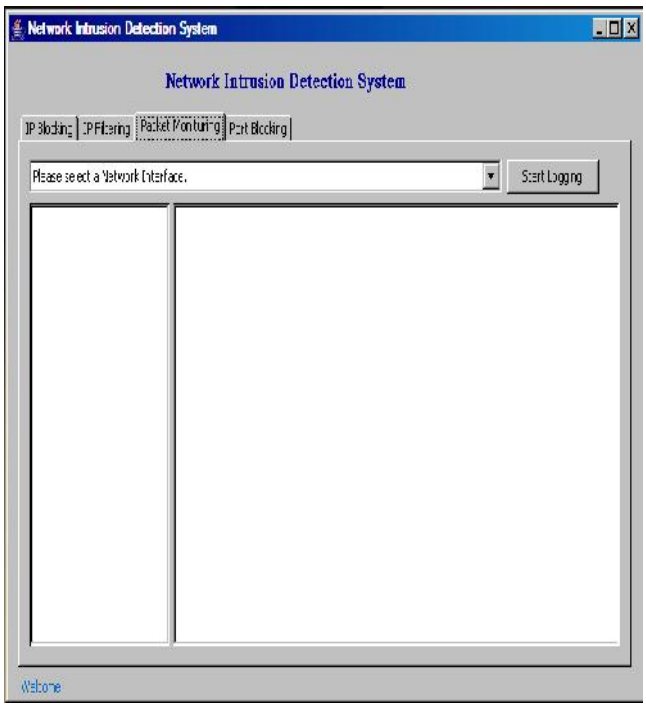
A button is used in Packet monitoring to start and stop the thread.

- **List box**:

A list box gives the option of a multiple selection in which we can select one option. In Packet monitoring, this box is used for showing the list of packets.

- **Text area:**

In Packet monitoring, text area is used for showing the content present in the packet which are present in the list box.



4. PORT BLOCKING:

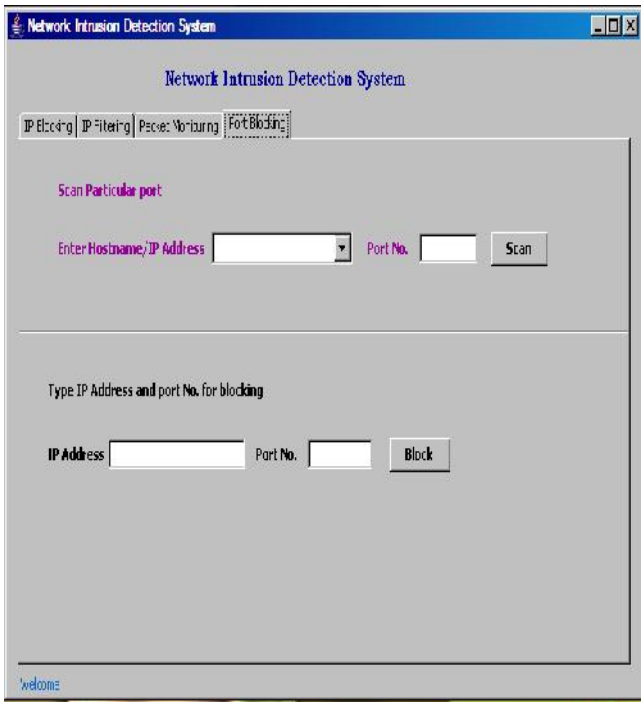
IP Blocking is separated into two parts: first one for scanning an IP address and second for blocking an IP address

- **Scanning of an IP address:**

In this block there is a text box for entering the IP address and its port number from which we have threat and a button scan for scanning that IP address and port number

- **Blocking of an IP address:**

In this block there is a text box for entering the IP address and its port number from which we have threat and a button block for blocking that IP address.



The ability to watch all the traffic in the network and provide security from hacker and crackers is the main goal of NIDS. There are many things IT professionals can and should do to protect network resources. Network IDS is just one of many tools that make up a bulletproof security strategy. Before implementing a network IDS solution, network managers need to realize that intrusion detection is neither a trivial task nor a panacea for every security woe. If implemented poorly, a network IDS might not monitor the appropriate traffic and completely miss an attack. By the same token, those who view the IDS as the end-all security tool may be lulled into a false sense of security, thinking that it’s doing something it was never configured to do.

CONCLUSION

Security is a very difficult topic. Everyone has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know why what's

been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.
Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

REFFERENCES

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.
[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.
[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.
[4] Sanchez-Avila, C. Sanchez-Reillol, R, —The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.
[5] Murat Fiskiran, Ruby B. Lee, —Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.
[6] Aameer Nadeem, Dr. M.Younus Javed, —A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.
[7] Pravin Wararkar and S.S. Dorle,"Performance Analysis Of Vehicular Adhoc Networks Handovers With Metaheuristic Algorithms:A Review", Sixth International Conference on Emerging Trends in Engineering and Technology,IEEE,2013.

[8]Pravin Wararkar and S.S. Dorle," Vehicular Adhoc Networks Handovers With Metaheuristic Algorithms", International Conference on Electronic Systems, Signal Processing and Computing Technologies,IEEE,2014.

[9]Pravin Wararkar and S.S. Dorle," Methodological Analysis of Inter VANET Data Handovers with Metaheuristic Algorithms", International Journal of Computer Applications (IJCA), Vol.130, No.12, pp.16-20, November 2015

[10]Pravin Wararkar and S.S. Dorle," Improving Handoff Addressing For IEEE 802.15.4 Based Vehicular Adhoc Networks (VANET's) By Particle Swarm Optimization (PSO)", International Journal of Research in Engineering and Applied Sciences(IJREAS-JREAS), Vol. 3, Issue 2, pp.94-101, July 2015

[11] Pravin Wararkar and S.S. Dorle," Transportation Security Through Inter Vehicular Ad-hoc Networks (VANETs) Handovers Using RF Trans Receiver", IEEE International Students' Conference on Electrical, Electronics and Computer Sciences ,IEEE,2016
[12]Pravin Wararkar and S.S. Dorle," Transportation Security Through Inter Vehicular Ad-hoc Networks (VANETs) Handovers Using RF Trans Receiver", IEEE International Students' Conference on Electrical, Electronics and Computer Sciences ,IEEE,2016