International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-4, April 2014

Scrutinizing the Art of Intrusion Detection

Abhay Limaye, Shraddha Kakne, Priti Tiple, Shubhangi Bhamare

Abstract— Internet services and applications have become an inextricable part of quotidian life, enabling communication and the management of confidential information from any place imaginable. These internet services are bound to be vulnerable to attackers. Billions of dollars are lost every year in mending the systems hit by the intrusions. The means for pinpointing and tracking these intrusions are called as Intrusion Detection Systems (IDS). Intrusion Detection Systems are procuring mainstream adulation as companies move more of their critical business interactions to the Internet. Thus, hereby, in this paper, we present the dissertation on the notion of Intrusion Detection wherein we first focus on the assorted genres of attacks or intrusions. Furthermore we attempt to discern the paradigm of Intrusion Detection Systems. Denouement of this paper elaborates pragmatic benefits and unrealistic conjectures of prevalent Intrusion Detection Systems.

Index Terms—Intrusion Detection System (IDS), Dos (Denial of Service), brute force Attack, SQL injection attack.

I. INTRODUCTION

Every day, criminals are invading countless homes and offices across the nation—not by breaking down windows and doors, but by breaking into laptops, personal computers, and wireless devices via hacks and bits of malicious code. Last year, a home or business in the United States was broken into every 11 minutes. Based on information coming from various response teams, during the last year, a computer was attacked or broken into more than once per second. The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country. These statistics maybe only the tip of the iceberg as companies develop the ability to identify and track break-ins. Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

The means for identifying and tracking break-ins is called "intrusion detection."Intrusion detection systems (IDS), which have long been a topic for theoretical research and development, are gaining mainstream popularity as companies move more of their critical business interactions to the Internet.

An intrusion detection system can provide advance knowledge of attacks or intrusion attempts by detecting an intruder's actions. In this respect, intrusion detection systems are a powerful tool in the organization's fight to keep its computing resources secure.

II. ASSORTED GENRES OF ATTACKS

A. Denial of Service

A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system.

Denial of service (DoS) attacks may be initiated from a single machine, but they typically use many computers to carry out an attack. Since most servers have firewalls and other security software installed, it is easy to lock out individual systems. Therefore, distributed denial of service (DDoS) attacks are often used to coordinate multiple systems in a simultaneous attack.

DoS attacks are a common method hackers use to attack websites. Since flooding a server with requests does not require any authentication, even a highly secured server is vulnerable. However, a single system is typically not capable of carrying out a successful DoS attack. Therefore, a hacker may create a botnet to control multiple computers at once. A botnet can be used to carry out a DDoS attack, which is far more effective than an attack from a single computer.

Denial of service attacks can be problematic, especially when they cause large websites to be unavailable during high-traffic times. Fortunately, security software has been developed to detect DoS attacks and limit their effectiveness. While many well-known websites, like Google, Twitter, and WordPress, have all been targets of denial of service attacks in the past, they have been able to update their security systems and prevent further service interruptions.

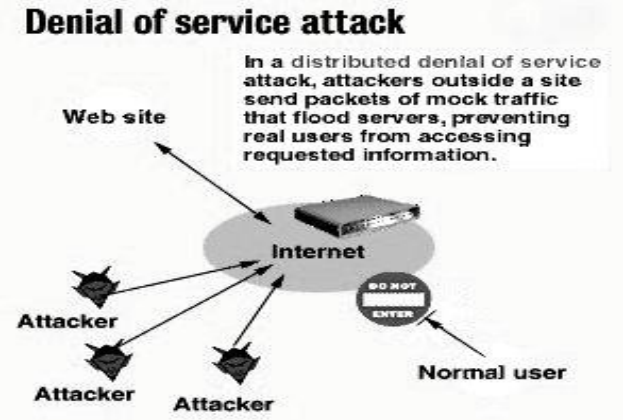

Fig.1 Overview of Denial of Service attack

Manuscript published on 30 April 2014.
* Correspondence Author (s)
Abhay Limaye*, Department of Computer Engineering Department, MIT College of Engineering, Pune - 411038, India.
Shraddha Kakne, Department of Computer Engineering Department, MIT College of Engineering, Pune - 411038, India.
Priti Tiple, Department of Computer Engineering Department, MIT College of Engineering, Pune - 411038, India.
Shubhangi Bhamare, Department of Computer Engineering Department, MIT College of Engineering , Pune - 411038, India.

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer
- Follow good security practices for distributing your email address. Applying email filters may help you manage unwanted traffic.

B. Brute Force Attack

A common threat Web developers face is a password-guessing attack known as a brute-force attack. A brute force attack is a trial-and-error method used to guess a person's user name, password, credit card number, or cryptographic key. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. If your Web site requires user authentication, you are a good target for a brute-force attack. An attacker can always discover a password through a brute-force attack, but the downside is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations. Hackers launch brute-force attacks using widely available tools that utilize wordlists and smart rulesets to intelligently and automatically guess user passwords. Although such attacks are easy to detect, they are not so easy to prevent.

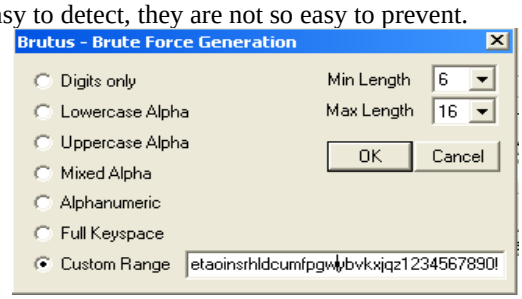

Fig.2 Brutus : A tool for Brute Force Generation

Example :

Brute Forcing Log-in Credentials

The most common type of a brute force attack in web applications is an attack against log-in credentials. Since users need to remember passwords, they often select easy to memorize words or phrases as passwords, making a brute force attack using a dictionary useful. Such an attack attempting to log-in to a system using a large list of words and phrases as potential passwords is often called a "word list attack" or a "dictionary attack". Attempted passwords may also include variations of words common to passwords such as those generated by replacing "o" with "0" and "i" with "1" as well as personal information including family member names, birth dates and phone numbers.

An attacker may try to guess a password alone or guess both the user name and the password. In the later case the attacker might fix the user name and iterate through a list of possible passwords, or fix the password and iterate through a list of possible user names. The second method, called a reverse brute force attack, can only get the credentials of a random user, but is useful when the attacked system locks users after a number of failed log-in attempts.

Types of Brute Force Attacks:

1.Dictionary attacks :Automated tools that try to guess user names and passwords from a dictionary file. A dictionary file might contain words that are gathered by the attacker to understand the user of the account about to be attacked, or to build a list of all the unique words available on the website.

2 .Search attacks :Covers all possible combinations of a character set and ranges of password length. This attack might take some time because of the large number of possible combinations.

3. Rule-based search attacks :Uses rules to generate possible password variations from part of a user name or from modifying pre-configured mask words in the input.

C. SQL Injection Attack

SQL Injection is one of the many web attack mechanisms used by hackers to steal data from organizations. It is perhaps one of the most common application layer attack techniques used today. It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database.

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution. SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. A SQL Injection attack is a form of attack that comes from user input that has not been checked to see that it is valid. The objective is to fool the database system into running malicious code that will reveal sensitive information or otherwise compromise the server.

SQL Injection is the hacking technique which attempts to pass SQL commands (statements) through a web application for execution by the backend database. If not sanitized properly, web applications may result in SQL Injection attacks that allow hackers to view information from the database and/or even wipe it out. Such features as login pages, support and product request forms, feedback forms, search pages, shopping carts and the general delivery of dynamic content, shape modern websites and provide businesses with the means necessary to communicate with prospects and customers.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

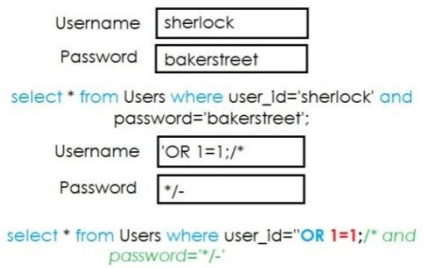

Fig.3 Example of SQL Injection Attack

Example:

Consider a simple login page where a legitimate user would enter his username and password combination to enter a secure area to view his personal details or upload his comments in a forum. When the legitimate user submits his details, an SQL query is generated from these details and submitted to the database for verification. If valid, the user is allowed access. In other words, the web application that controls the login page will communicate with the database through a series of planned commands so as to verify the username and password combination. On verification, the legitimate user is granted appropriate access.

Through SQL Injection, the hacker may input specifically crafted SQL commands with the intent of bypassing the login form and seeing what lies behind it. This is only possible if the inputs are made invulnerable and sent directly with the SQL query to the database. SQL Injection vulnerabilities provide the means for a hacker to communicate directly to the database. The technologies vulnerable to this attack are dynamic script languages including ASP, ASP.NET, PHP, JSP, and CGI. All an attacker needs to perform an SQL Injection hacking attack is a web browser, knowledge of SQL queries and creative guess work to important table and field names.

D. Privilege Escalation Attack

Privilege escalation is the act of exploiting a bug, designing flaw or configuration oversight in an operating system or say software application to gain access to the resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developers that can perform unauthorized actions. A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.

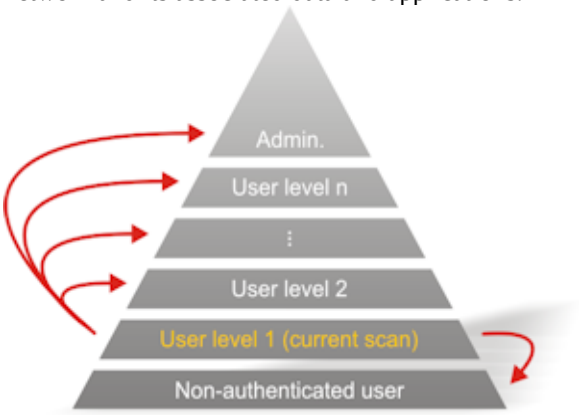

Fig.4 pictorial view of privilege escalation attack

Not every system hack will initially provide an unauthorized user with full access to the targeted system. In those circumstances privilege escalation is required. There are two kinds of privilege escalation: vertical and horizontal. In vertical privilege escalation, a user has administrative access to a computer when this should not be possible. Such access can allow users to change system settings, create new users, authorize activities, and engage in a wide variety of other mischief. This can be a potentially serious security flaw on a network, where a user with administrative privileges could extract data from the computers of network users or create loopholes to exploit later. Horizontal cases of privilege escalation involve situations where people have access controls under the account of a different user. In an office, for example, User A could access User B's account. Both accounts may have the same number of system privileges in terms of being able to make changes and perform operations. They contain different information, however, and User A could do things like deleting or moving files, accessing confidential information, or issuing orders under User B's name.

III. INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is composed of hardware and software elements that work together to find unexpected events that may indicate an attack will happen, is happening, or has happened. Note that we must think in all three tenses; some products warn in advance that an attack may take place, some warn as they notice an attack in progress, and some warn when they notice the aftereffects of the attack.IDS examines system or network activity to find possible intrusions or attacks. Intrusion detection systems are either network-based or host-based; vendors are only beginning to integrate the two technologies.

IDS determines suspicious behavior using following three kinds of commercially available analysis engines:

- Event or Signature-based Analysis
- Statistical Analysis
- Adaptive Systems

The event, or signature-based, systems function much like the anti-virus software with which most people are familiar. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack; the IDS merely scans the environment looking for a match to the known patterns. The IDS can then respond by taking a user-defined action, sending an alert, or performing additional logging. This is the most common kind of intrusion detection system. A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, then looks for deviations from “normal”. After over 10years of government research, some products are just beginning to incorporate this technology into marketable products. The adaptive systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the system understands how people interact with the environment, and then warn operators about unusual activities. There is a considerable amount of active research in this area.

IV. NETWORK IDS

The network IDS usually has two logical components: the sensor and the management station.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator. The sensors are usually dedicated systems that exist only to monitor the network. They have an network interface in promiscuous mode, which means they receive all network traffic, not just that destined for their IP address, and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station. The analysis station can display the alarms or do additional analysis. Some displays are simply an interface to a network management tool, like HP Open view, but some are custom GUIs designed to help the operator analyze the problem.

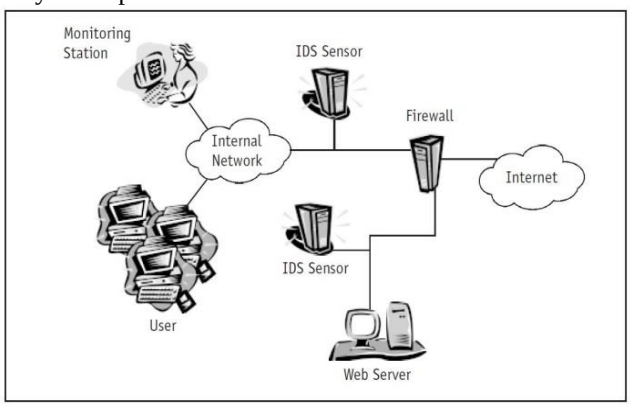

Fig.4This diagram shows placement of a traditional network based IDS with two sensors on separate network segments that communicate with a monitoring station on the internal network.

Strengths

The network intrusion detection systems can detect some of the attacks that use the network. They are good for detecting access without authority or some kinds of access in excess of authority. A network-based IDS does not require modification of production servers or hosts. This is an advantage because production servers frequently have close operating tolerances for CPU, I/O, and disk capacity; installing additional software may exceed the systems capacities. The IDS is not on a critical path for any production services or processes because a network-based IDS does not act as a router or other critical device. System failure does not have a significant impact on the business. A side benefit of this is that you are likely to encounter less resistance from other people within your organization; the risk to existing critical processes is lower with a network system than with a host system.

Network-based IDS systems tend to be more self-contained than host-based systems. They run on a dedicated system that is simple to install; merely inbox the device, do some remedial configuration, and plug it into your network in a location that permits it to monitor sensitive traffic.

Weaknesses

A network based IDS, on the other hand, only examines network traffic on the segment to which it is directly connected, but it cannot detect an attack that travels through a different network segment. This problem—localized vision—is particularly endemic in a switched Ethernet environment. The problem may require that an organization purchase many sensors in order to meet their network coverage goals. Since each sensor costs money, broad coverage with network IDS sensors can become prohibitively expensive.

Network intrusion detection systems tend to use signature analysis in order to meet performance requirements. This will detect common programmed attacks from external sources, but it is inadequate for detecting more complex information threats. This requires a more robust ability to examine the environment.

A network intrusion detection system may need to communicate large volumes of data back to the central analysis system. Sometimes that means that any given monitored packet generates a larger amount of analysis traffic. Many such systems use aggressive data-reduction processes to reduce the amount of communicated traffic. They also push much of the decision-making processes out into the sensor itself and use the central station as a status display or communications center, rather than for actual analysis. The disadvantage of this is that it provides very little coordination amongst sensors; any given sensor is unaware that another has detected an attack. Such a system cannot normally detect synergistic or complex attacks.

A network-based IDS may have a difficult time handling attacks within encrypted sessions. Fortunately, there are very few attacks that take place within an encrypted traffic session, other than attacks against weak web servers. This will become more often issue as organizations transition to IPv6.

V. HOST IDS

The host-based IDS looks for signs of intrusion on the local host system. These frequently use the host system's audit and logging mechanism as a source of information for analysis. They look for unusual activity that is confined to the local host such as logins, improper file access, unapproved privilege escalation, or alterations on system privileges. This IDS architecture generally uses rule-based engines for analyzing activity; an example of such a rule might be, "super user privilege can only be attained through the subcommand." Therefore successive login attempts to the root account might be considered an attack.

VI. FILE INTEGRITY CHECKERS

A file integrity checker examines the files on a computer to determine whether they have been altered since the last time the integrity checker was run. The integrity checker keeps a database of hash values for each file. Each time the checker runs, it recalculates the hash value and compares it to the stored value. If the hash values are different, the file has changed. If the values are not different, the file has not changed.

VII. VULNERABILITY SCANNERS

A vulnerability scanner differs from an intrusion detection system, as mentioned earlier, in that the vulnerability scanner looks for static configurations and the IDS looks for transient misuse or abnormalities. A vulnerability scanner may look for a known NFS vulnerability by examining the available services and configuration on a remote system. An IDS, handling the same vulnerability, would only report the existence of the vulnerability when an attacker attempted to exploit it.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Vulnerability scanners, whether network or host scanners, give the organization the opportunity to fix problems before they arise, rather than reacting to an intrusion or misuse that is already in progress. An intrusion detection system detects intrusions in progress, while a vulnerability scanner allows the organization to prevent the intrusion in the first place. Vulnerability scanners may be helpful in organizations without a good incident response capability.

VIII. NETWORK VULNERABILITY SCANNER

A network vulnerability scanner operates remotely by examining the network interface on a remote system. It will look for vulnerable services running on that remote machine, and report on a possible vulnerability. For example, it is well-known thatrexd is a weak service; a network vulnerability scanner will attempt to connect to therexd service on the target system. If the connection succeeds, the scanner will report rexd vulnerability.

Since a network vulnerability scanner can be run from a single machine on the network, it can be installed without impacting the configuration management of other machines. Frequently, these scanners are used by auditors and security groups because they can provide an "outsider's view" of security holes in a computer or network.

IX. HOST VULNERABILITY SCANNER

A host vulnerability scanner differs from a network vulnerability scanner in that it is confined entirely to the local operating system. A network vulnerability scanner requires the target machine be accessible from the network in order for it to operate; a host vulnerability scanner does not. Host vulnerability scanners are software packages that are installed on particular operating systems. Once the software is installed it can be configured to run at anytime of the day or night. Usually the scans performed by this type of tool are scheduled to run at a low priority to reduce the impact of the scan on production work.

X. PRAGMATIC PERKS OF IDS

1. They can lend a greater degree of integrity to the rest of your security infrastructure. Intrusion detection systems provide additional layers of protection to a secured system. The strategy of a system attacker will often include attacking or otherwise nullifying security devices protecting the intended target. Intrusion detection systems can recognize these first hallmarks of attack, and potentially respond to them, mitigating damage. In addition, when these devices fail, due to configuration, attack, or user error, intrusion detection systems can recognize the problem and notify the right people.
2. They can make sense of often obtuse system information sources, telling you what's really happening on your systems. Operating system audit trails and other system logs are a treasure trove of information about what's going on internal to your systems. They are also often incomprehensible. Intrusion detection systems allow administrators and managers to tune, organize, and comprehend what these information sources tell them, often revealing problems before loss occurs.
3. They can trace user activity from the point of entry to point of exit or impact. In the unlikely event that an intruder gets past a perimeter defense device, such as a firewall, an IDS provides a way to catch his actions. In addition, an IDS can detect the actions of a "bad guy" already on the inside—an attack from an insider or via a previously unknown entry path to the network.
4. They can recognize and report alterations to critical system and data files. File integrity assessment tools utilize strong cryptographic checksums to render these files tamper-evident and, in the case of a problem, quickly ascertain the extent of damage.
5. They can spot errors of your system configuration that have security implications, sometimes correcting them if the user wishes. Vulnerability assessment products allow consistent auditing and diagnosis of system configuration settings that might cause security problems.

XI. UNREALISTIC CONJECTURES

1. They are not magic bullets. Security is a complex area with myriad possibilities and difficulties. In networks, it is also a "weakest link" phenomenon—i.e., it only takes one vulnerability on one machine to allow an adversary to gain entry and potentially wreak havoc on the entire network. The time it takes for this to occur is also minuscule. There are no magic solutions to network security problems, and intrusion detection products are no exception to this rule. However, as part of a comprehensive security management they can play a vital role in protecting your systems.
2. They cannot compensate for weak identification and authentication mechanisms. We must still rely on strong identification and authentication of users. A security infrastructure that includes strong I&A and intrusion detection is stronger than one containing only one or the other.
3. They cannot conduct investigations of attacks without human intervention. One must perform incident handling. One must investigate the attacks, determine, where possible, the responsible party, then diagnose and correct the vulnerability that allowed the problem to occur, reporting the attack and particulars to authorities where required.
4. They cannot intuit the contents of your organizational security policy. Intrusion detection expert systems increase in value when they are allowed to function as both hacker/burglar alarms and policy-compliance engines.
5. They cannot compensate for problems in the quality or integrity of information the system provides. In other words, "garbage in garbage out" still applies.
6. They cannot analyze all of the traffic on a busy network. Network-based intrusion detection is capable of monitoring traffic of a network, but only to a point. First, given the vantage-point of network-based intrusion detection sources that rely on network adapters set to promiscuous mode, not all packets are visible to the systems. Second, as traffic levels rise, the associated processing load required to keep up becomes prohibitive and the analysis engine either falls behind or fails.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7. They cannot always deal with problems involving packet-level attacks. There are weaknesses in packet-capture-based network intrusion detection systems. The heart of the vulnerabilities involves the difference between the IDS's interpretation of the outcome of a network transaction (based on its reconstruction of the network session) and the destination node for that network session's actual handling of the transaction. Therefore, a knowledgeable adversary can send series of fragmented and otherwise doctored packets that elude detection, but launch attacks on the destination node. Worse yet, an adversary can use this sort of packet manipulation to accomplish a denial of service attack on the IDS itself by overflowing memory allocated for incoming packet queues.

XII. CONCLUSIONS

Intrusion detection currently attracts considerable interest from both the research community and commercial companies. Research prototypes continue to appear, and commercial products based on early research are now available. In this paper, we have given an overview of the current state of the art of intrusion detection. Many methods preventing intrusion into computer systems have been implemented, but these will always be imperfect. An automated system for detecting anomalous user behavior will help alleviate a, sometimes unrealistic, burden on systems administrators. However, these automated systems are not only useful during a violation but can be an invaluable forensic tool after the fact.

XIII. ACKNOWLEDGMENT

We thank our college MIT College of Engineering Pune for giving us the opportunity for doing this survey. We also would like to thank our project guide Prof .Sharmishtha Desai for helping us during this whole process.

REFERENCES

[1] Amrita Anand,Brajesh Patel"International Journal of Advanced Research in Computer Science and Software Engineering",International Journal of Advenced Research in Computer Science and Software Engineering 2 (8), August- 2012.

2] Sapna S. Kaushik, Dr.Prof.P.R.Deshmukh"Detection of Attacks in an Intrusion Detection System" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011

[3] Renaud Bidou "Denial of Service Attacks"

[4] John Bellardo and Stefan Savage "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions"

[5] Faizal, M.A., MohdZaki M., Shahrin Sahib, Robiah, Y., SitiRahayu, S., and AsrulHadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

[6] Christopher Kruegel, Fredrik Valeur, Giovanni Vigna(2005). Intrusion Detection and Correlation, Challenges and Solution, Springer Science+Business Media Inc, USA.