A

Seminar report

On

Intrusion Detection Systems

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **Intrusion Detection Systems**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least,I would thank The Almighty for giving me strength to complete my report on time.

INDEX

INTRODUCTION

INTRUSION DETECTION SYSTEM

Intrusion is some time also called as hacker or cracker attempting to break into or misuse your system. While introducing the concept of intrusion detection in 1980, defined an **intrusion attempt** or a **threat** to be the potential possibility of a deliberate unauthorized attempt to

- access information,
- manipulate information, or
- Render a system unreliable or unusable.

Intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

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. An IDS installed on a network provides much the same purpose as a burglar alarm system installed in a house. Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert.

HISTORY

A computer system should provide *confidentiality*, *integrity* and *assurance* against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. So IDS come in to existence.IDS provides all facilities to protect your system.

Intrusion Detection (ID) defined:

Process of monitoring computer networks and systems for violations of security policy

First ID System--manual "system audits" 1980, ID was born

Government sponsored development in early 1980's. First ID systems for Air Force and Navy.

First document need for automated audit trail review to support security goals.

As the Growth of Internet force IDS to be developed.

Commercial ID systems began appearing in early 1990's

DEALING WITH INTRUDRES

Due to increase connectivity (more specially on internet),and much chances of financial possibility that are opening more and more system are subject to attack by intruders(intruders are the hacker or cracker those are unauthorised usres),because completelt secure system is still a dream.

Firewall and filterring router are not enough to protect electronic assets.so detection is needed. In terms of the relation intruder-victim, attacks are categorized as:

-**External Intruders**: who are unauthorised usres of the machines they attack,they coming from outside, frequently via the Internet.they can be any person which are not in our knowledge.

-**Internal Intruders**: who has permission to access system but not some portion of it, they coming from own enterprise's employees or their business partners or customers.

further subdivided:

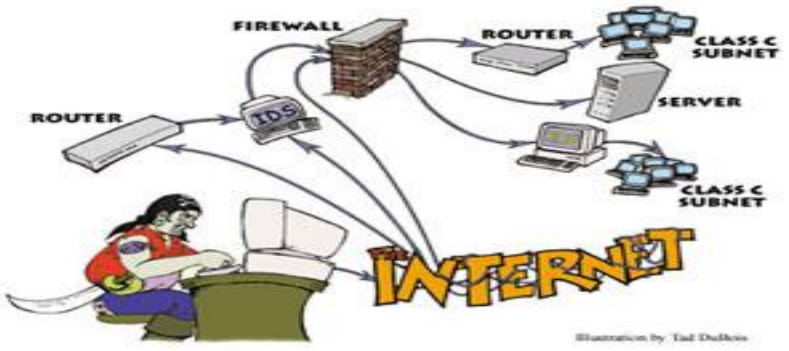
-**Masquerade**: Those user who masquerade another user means using others usre no or identification no access the non permitted information.

-**Legitimate**:Those user who legally access the information but they are not allowed to access information.but using some kind of techniques they able to access sensitive data legally.They are most dangerous type.

-**Clandestine**:User who have power to turnoff audit control for them selves and steal information.

HOW DOES IDS WORK?

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts.



In terms of response IDS classified as:

- **passive system**: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert
- **Reactive system.** In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Types of IDS

Basically IDS are of two type's i.e.

--NIDS (**Network Intrusion Detection Systems)**

--HIDS (**Host Intrusion Detection Systems**)

Both of them has their own prone and cons. let us discuss both of them one by one.

Network Intrusion Detection Systems

A network IDS (NIDS) monitors all traffic on the network segment that it is placed on. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments can't be monitored unless the traffic is directed to the NIDS promiscuous interface.

Network Intrusion Detection involves looking at the packets on the network as they pass by the NIDS. The NIDS can only see the packets that are carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature or certain behavior. Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic; however doing so might create a bottleneck that would impair the overall speed of the network.

Host Based Intrusion Detection Systems

A Host IDS (HIDS) uses a piece or pieces of software on the system to be monitored. The loaded software uses log files and/or the system's auditing agents as sources of data. In contrast, a NIDS monitors the traffic on its network segment as a data source.

Host based intrusion detection involves not only looking at the network traffic in and out of a single computer, but also checking the integrity of your system files and watching for suspicious processes. To get complete coverage at your network with HIDS, you must load the software on every computer. Host based Intrusion Detection is much more effective in detecting insider attacks than is NIDS. Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

The below diagram shows a HIDS.

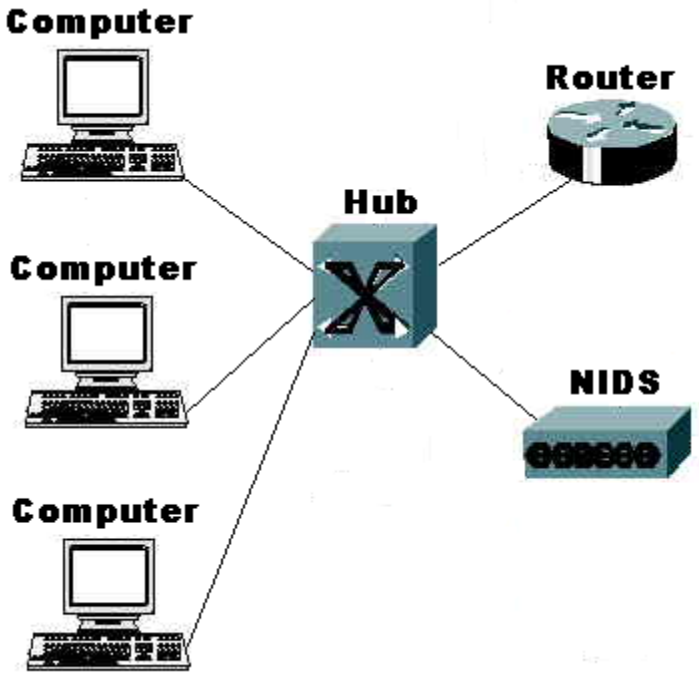


Fig . 1: HIDS

HIDS vs NIDS

- **Unauthorized outsider access:** When an unauthorized user logs in successfully, or attempts to log in, they are best tracked with host-based IDS. However, detecting the unauthorized user before their log on attempt is best accomplished with network-based IDS.
- **Bandwidth theft/denial of service:** These attacks from outside the network single out network resources for abuse or overload. The packets that initiate/carry these attacks can best be noticed with use of network-based IDS.
- **Traffic monitors:** NIDS monitors all traffic on a network segment & can detect intrusion that crosses a specific network segment. It will not see traffic that passes between LAN computers. Whereas a HIDS examines all traffic and activity for a particular machine and can detect system log files as well as inbound and outbound packets. Each system is requiring its own IDS.

HIDS and NIDS Used in Combination

The two types of intrusion detection systems differ significantly from each other, but complement one another well. The best IDS tools combine both approaches under one management console. That way, the user gets comprehensive coverage, making sure to guard against as many threats as possible.

IDS Techniques

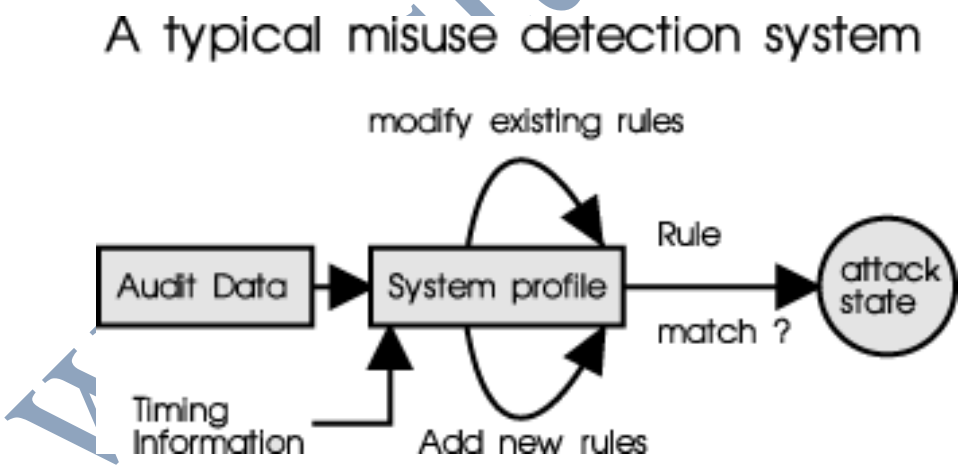
Now that we have examined the two basic types of IDS and why they should be used together, we can investigate how they go about doing their job. For each of the two types, there are two basic techniques used to detect intruders:

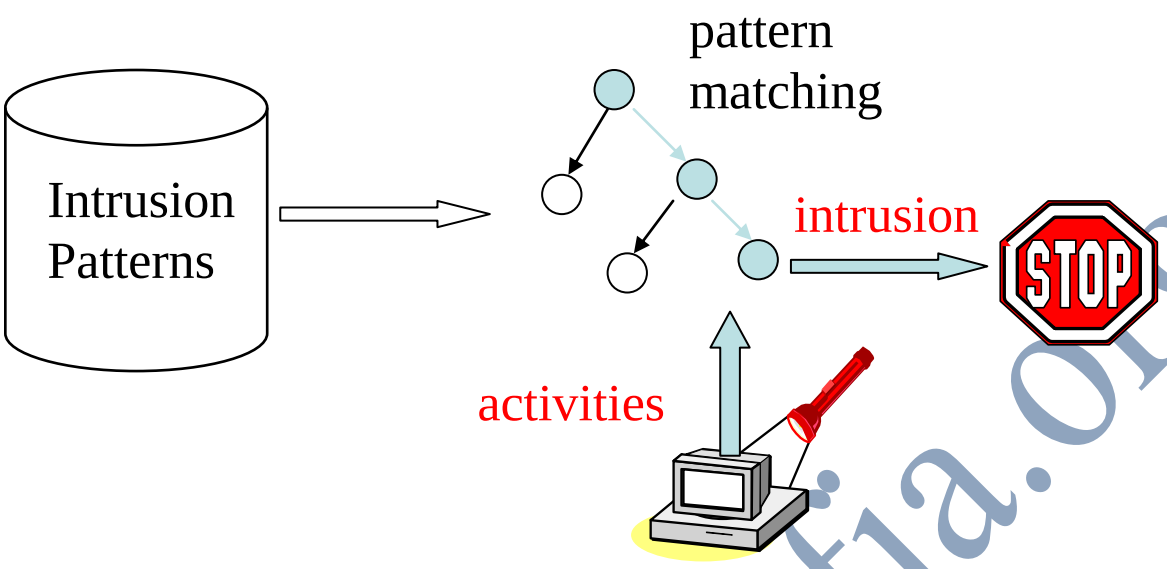
Misuse detection (Signature detection or Pattern Detection).

Anomaly detection (Behavior detection)

Misuse Detection or Signature based IDS or Pattern Detection

Almost all IDSs are signature based, also known as knowledge based. Signature based IDSs monitor network traffic and analyzes this traffic against specific predefined attacks. When an attack is detected an alarm is generated. This means that any traffic that doesn't specifically match a signature is considered safe. Signature based IDSs obviously require that the signature base be updated regularly to detect new exploits. If legitimate network traffic triggers an alarm this is called a false positive. The amount of false positives generated by signature based IDSs can be significantly less than behavior based IDSs.





A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Behavior based IDS or Abnormal behavior

It does what its name describes. It looks for abnormal behavior. How is this different from suspicious detection? Here is an example; most corporate LANs are only active during business hours. From 9 AM - 6 PM, the servers are active, users are logged on, and the routers are busy. However, during non-business hours, the network should be rather stagnant. This is where the abnormal IDS come into play. In the event that a workstation on your network is infected with a Trojan, the hacker could use that machine to gain access to the rest of your network including the file servers. Usually, this is late at night when the administrator and users won't notice. Abnormal IDS would record network activity and file requests during non-business hours. So, if a user was all of the sudden requesting files from server at 2 AM, the abnormal detection IDS would send a red flag. This allows network administrators to know exactly what is going on when they

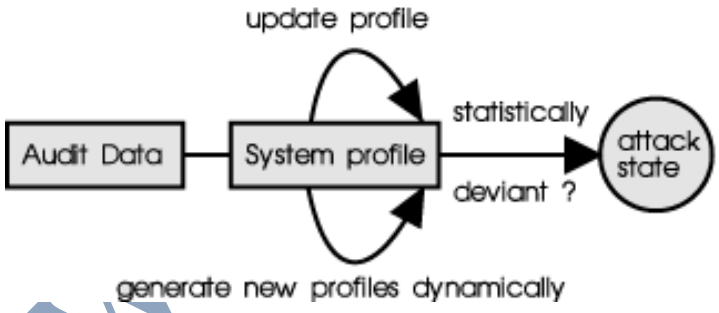
are not there.

Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive.

Advantages of behavior-based approaches are that they can detect attempts to exploit new and unforeseen vulnerabilities. They can even contribute to the automatic discovery of these new attacks. They also help detect 'internal abuse' types of attacks that do not actually involve exploiting any security vulnerability.

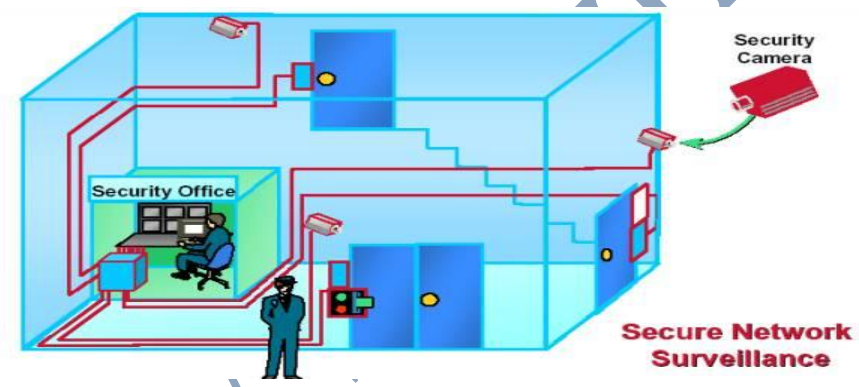
An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline wills an example of this would be if a user logs on and off of a machine 20 times a day instead of the normal 1 or 2. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions.

A typical anomaly detection system



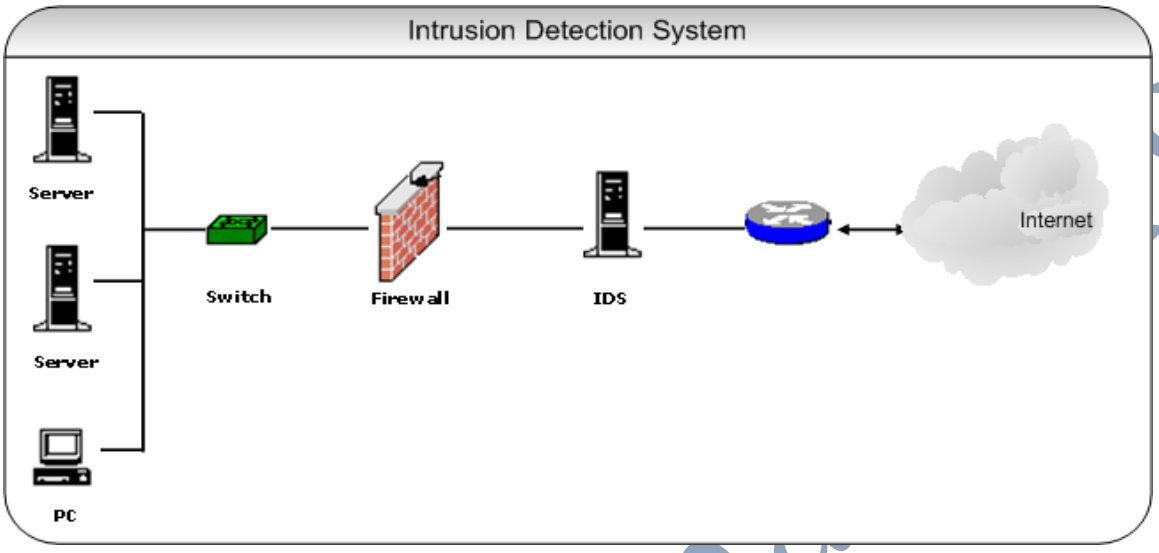
Firewall vs. IDS

Although IDSs may be used in conjunction with firewalls, which aim to regulate and control the flow of information into and out of a network, the two security tools should not be considered the same thing. Using the previous example, firewalls can be thought of as a fence or a security guard placed in front of a house. They protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety. most firewalls never alert an administrator. The administrator may notice if he/she checks the access log of the firewall, but that could be weeks or even months after the attack. This is where an IDS comes into play.



- Firewall cannot detect security breaches associated with traffic that does not pass through it. Only IDS is aware of traffic in the internal network
- Not all access to the Internet occurs through the firewall.
- Firewall does not inspect the content of the permitted traffic
- Firewall is more likely to be attacked more often than IDS
- Firewall is usually helpless against tunneling attacks
- IDS is capable of monitoring messages from other pieces of security infrastructure

Whereas a firewall may be used in both home and commercial environments, Intrusion Detection Systems are only really feasible within commerce.



The combination of the Intrusion Detection System and a firewall will allow maximum filtering of network traffic and will definitely prevent the majority of attacks.

Some reasons for adding IDS to you firewall are:

- Double-checks misconfigured firewalls.
- Catches attacks that firewalls legitimate allow through (such as attacks against web servers).
- Catches attempts that fail.
- Catches insider hacking.

Benefits of IDS

- Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms.
- Allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs.
- Can make the security management of systems by non-expert staff possible by providing nice user friendly interface.
- Comes with extensive attack signature database against which information from the customers system can be matched.
- Can recognize and report alterations to data files.
- It provides time to time information, it recognize attacker (intrusion) & report alteration to data files.
- IDS generate alarm and report to administrator that security is breaches and also react to intruders by blocking them or blocking server.

IDS is not a *SILVER BULLET*

- Cannot conduct investigations of attacks without human intervention.
- Cannot intuit the contents of your organizational security policy.
- Cannot compensate for weaknesses in network protocols.
- Cannot compensate for weak identification and authentication mechanisms.
- Capable of monitoring network traffic but to a certain extent of traffic level.
- It can neither tell you exactly who and how the attack occurred nor the intention of the attacker.

CONCLUSION

As security incidents become more numerous, IDS tools are becoming increasingly necessary. They round out the security arsenal, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity

- **IDS have come a long way**
  - **Still a long way to go**
- **Many different products on the market**
- **Many different uses**
- **Open source solutions are very popular**
- **No easy or long-term solution to network security**
  - **Vigilance will have to be maintained**

Intrusion detection systems add an early warning capability to your defenses, alerting you to any type of suspicious activity that typically occurs before and during an attack. Since most cannot stop an attack, intrusion detection systems should not be considered an alternative to traditional good security practices. There is no substitute for a carefully thought out corporate security policy, backed up by effective security procedures which are carried out by skilled staff using the necessary tools. Instead, intrusion detection systems should be viewed as an additional tool in the continuing battle against hackers and crackers.

REFERENCES

- **www.securityfocusonline.com/IDS**
- **www.linuxsecurity.com/4030/topic/IDS**
- **www.netsecurity.about.com**
- **www.acm.com/intrusion detection system/**
- **www.securitydocs.com**
- **www.studymafia.org**