ISSN 2250-3153

Security of Network Using Ids and Firewall

Kanika, Urmila

M.TECH (Computer Science & Engneering)

Abstract- An intrusion detection system (IDS) detects intruders that is, unexpected, unwanted or unauthorized people or programs on computer network. An IDS is used to determine if a computer network or server has experienced an unauthorized intrusion. An IDS works like a burglar alarm system. If it detects a possible intrusion, the IDS system will send out an alert or warning which would prompt an administrator to perform further investigation which might include computer forensics and prosecution.

Index Terms- IDS is Intrusion Detection Sytem, NIDS is Network based Intrusion Detection System, HIDS is Host based Intrusion Detection System.

I. INTRODUCTION

IDS is a security countermeasure. It monitors things looking for signs of intruders. An IDS monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. IDS is any hardware, software, or a combination of both that monitors a system or network of systems against any malicious activity. This is mainly used for detecting break-ins or misuse of the network. In short, we can say that IDS is the 'burglar alarm' for the network because much like a burglar alarm, IDS detects the presence of an attack in the network and raises an alert. An IDS provides three functions: monitoring, detecting and generating an alert. IDS is a system that will constantly monitor the corporate networks from all types of attacks and vulnerabilities. IDS looks for the attack signatures which are specific patterns that usually indicate malicious or suspicious event.

II. NEED OF IDS

Intrusion detection describes the intention - not the methodology. A network firewall will keep the bad guys off the network and anti-virus will recognize and get rid of any virus and password-protected access control will stop the office cleaner trawling through the network after we have gone.So that's it – we are fully protected. But we are wrong because a firewall has got holes to let things through: without it, you wouldn't be able to access the Internet or send or receive emails. Anti-virus systems are only good at detecting viruses they already know about. And passwords can be hacked or stolen .That's the problem. We can have all this security, and all we have really got is a false sense of security. If anything or anyone does get through these defenses, through the legitimate holes, it or they can live on your network, doing whatever they want for as long as they want. And then there's a whole raft of little known vulnerabilities, known to the criminals, who can exploit them and gain access for fun, profit or malevolence. A hacker will quietly change your system and leave a back door so that he can come and go undetected whenever he wants. A Trojan might be designed to hide itself, silently gather sensitive information and secretly mail it back to source. And we won't even know it's happening because we will believe it can't be happening because we have got a firewall, anti-virus and access control.

Unless, that is, you also have an intrusion detection system (IDS). While those other defenses are there to stop bad things getting onto your network, an IDS is there to find and defeat anything that might just slip through and already be on your system. And in today's world, you really must assume that things will slip through – because they most certainly will. From the outside, you will be threatened by indiscriminate virus storms; from hackers doing it for fun (or training); and more worryingly from organized criminals specifically targeting you for extortion, blackmail or saleable trade secrets. From the inside, you will have walk-in criminals using social engineering skills to obtain passwords to, or even use of, your own PCs; from curious staff who simply want to see what their colleagues are earning and from malcontents with a grievance.

III. IDS FUNCTIONALITY

Intrusion Detection System (IDS) is an essential tool that compliments any security suite such as a firewall and a good antivirus. These tools are ineffective if used separately as each one is tailored to fight off attackers in specific focused areas. It is good practice to build a security suite with well recognized reliable technologies that have been tried and tested, ensuring that the IDS application chosen suits your organizations needs closely like a well tailored piece of clothing. Many network security professionals know that a firewall is an essential element to a comprehensive security plan. It is also felt that IDS is an excellent complementary product that will complete the company's security strategy. What many security professionals overlook is the type of IDS that best fits the organization.

An IDS system is used to make security professional aware of packets entering and leaving the monitored network. IDS are often used to sniff out network packets giving you a good understanding of what is really happening on the network. There are two mainstream options when implementing **IDS Host based IDS and Network based IDS**. IDS have the ability to drop malicious packets that may cause your network harm. This is the latest technological advance on firewalls and because the IDS have pattern files you can be certain that the latest network bug will be swatted from your LAN, WAN, WLAN.IDS Systems have the capability of dropping potentially damaging packets that have been identified in a similar way that antivirus manufactures detect viruses. All packets that pass though the IDS are analyzed

and compared against a pattern or signature file that verifies that the packet is not an attack on the network integrity. If the packet is dropped the IDS can be configured to log this event and notify the security professional immediately so action can be taken against the attacker.

1. NIDS (network intrusion detection system)

NIDS are placed in key areas of network infrastructure and monitors the traffic as it flows to other host. An NIDS should best be describes as a standalone appliances that has network intrusion detection capabilities. A NDIS is a software package that you install on dedicated workstation that is connected to your network or a device that has the software embedded and is also connected to your network. The NIDS then scans any traffic that is transmitted over that segment of your network. The NIDS functions in very much the same way as high-end antivirus applications and it makes use of signature or pattern file method comparing each transmitted packet for patterns that may occur within the signature file. The IDS functions in a very conform way in order to increase packet throughput as inspecting every packet can slow traffic considerably. An IDS then uses the firewall approach when inspecting the packet by letting through the packets that are not potentially dangerous. This processing is done by the IDS's preprocessing filters that arranges that data that is scanned.

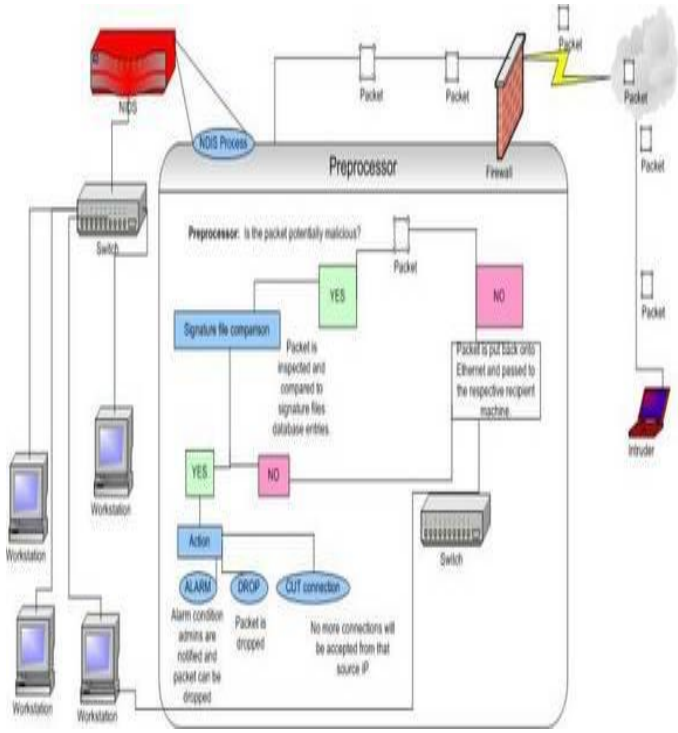

Fig1.The diagram above emulates the NIDS system; it shows the process of how the NIDS compares the potential intruder packet with the rule list and signature files that are stored within the NIDS database.

2. HIDS (Host intrusion detection system)

Intrusion Detection System is installed on a host in the network. HIDS collects and analyzes the traffic that is originated or is intended to that host. Host intrusion detection systems are installed locally on host machines making it a very versatile system compared to NIDS. HIDS can be installed on many different types of machines namely servers, workstations and notebook computers. Doing so gives you the edge that NIDS does not have especially if you have a segment that you NDIS can not reach beyond. Traffic transmitted to the host is analyzed and passed onto the host if there are not potentially malicious packets within the data transmission. HIDS are more focused on the local machines changing aspect compared to the NIDS. NIDS focus more greatly on the network those specific hosts themselves.

IV. COMPARITIVE ANALYSIS OF HIDS VS. NIDS

Do we need a NIDS or a HIDS? The answer is HIDS for a complete solution and NDIS for a LAN solution. When administering an HIDS solution we found it to require significantly less specialist knowledge while NIDS required undivided attention and after Lab setups the team got NIDS working. HIDS has more logging than NIDS when taking into account that HIDS logs all machines on the network. If you have LAN bandwidth constraints it is very feasible to look at a HIDS. If price is an issue I found that some NIDS solutions are considerably more expensive when compared to a HIDS solution as there is a capital outlay on the hardware and some vendors charge considerably more for the software. The **NIDS** handle security at the network level. The **HIDS** handle security at the host level. An NIDS needs dedicated hardware, and forms a system which can check packets traveling on one or more network lines, in order to find out if any malicious or abnormal activity has taken place. The H-IDS resides on a particular host, and its software therefore covers a broad range of operating systems, such as Windows, Solaris, Linux, HP-UX, Aix, etc

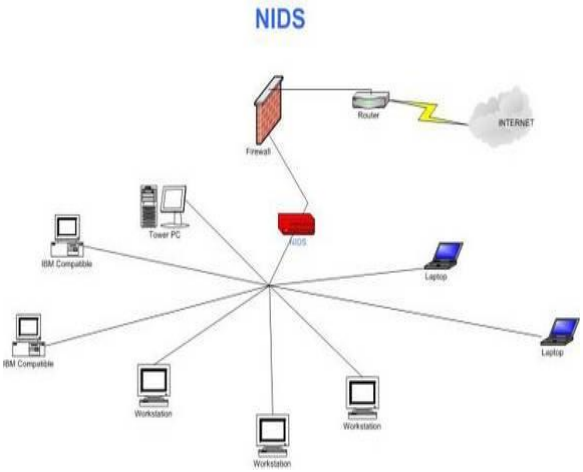

Fig2. Network Based Intrusion Detection System

The diagram above represents the typical NIDS scenario where an attempt has been made to funnel the traffic through the NIDS device on the network. It does not take a genius to see that if you had to isolate a single machine and take the machine away from the network like is done by many business people when in

transit that NIDS would be very flawed. The Red device represents where the NIDS has been installed.

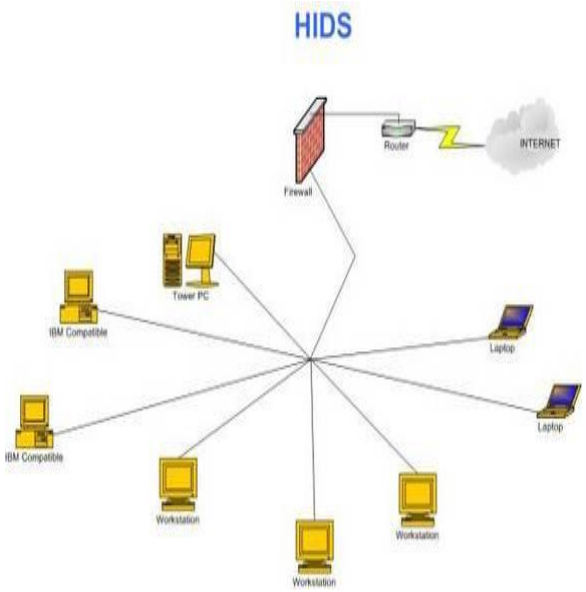

Fig3.Host Based Intrusion Detection System

Host based IDS are a more comprehensive solution and displays great strengths in all network environments. It does not matter where the machines are even if they are away from the network they will be protected at all times. The Orange machines represent where the HIDS is installed.

V. PREVENTING AND DETECTING INSIDER ATTACKS USING IDS

Insider Attacks are an unusual type of threat. Unlike external attacks, the intruder is someone who has been entrusted with authorized access to the network. In fact, the attacker requires access in order to fulfill their obligations to the victim organization. Furthermore, they often have a substantial amount of knowledge about the network architecture, including where their targeted files or systems are located. Because many organizations' security is focused on protecting the perimeter of the network, little attention is paid to what is occurring within the system. As a result, insider attacks may not be discovered for months after the attack, long enough for the perpetrator to get off scot-free. Creating a good rule set for the internal IDS. The reason the rule set needs to be different is due to the fact that different network users require a different amount of access to different services, servers, and systems for their work. The rule set of the internal IDS system should be created so that all the static of employees' day-to-day work activities, such as accessing various services and servers, does not trigger attack warnings, and only the important information is reported. This important information would include detected activities that users do not require for their daily work, as well as any other glaringly obvious attacks. The logging and reporting of attacks by the internal IDS systems can be used to do much more than detect specific, isolated, and unrelated attacks. By combining the data from all internal IDS systems, system administrators can identify attack trends and patterns. Once attack trends and patterns are identified, the admins will be more able to identify any network users who pose a threat to network security, have been exhibiting any malicious network behavior, or who are doing anything that is against company policy in general. Once these users have been identified, the proper action can be taken to prevent any successful intrusions or the continuance of the activity.

Further, the logs provided by IDS systems can allow the system administrators an audit trail in case there are in fact any successful intrusions. Identified attack trends and patterns can also allow system administrators to see where people are trying to attack against the most. This would allow them to identify any possible security holes, or policy oversights, as well as any servers on the network that have a higher risk of being attacked, and thus allow them to know which systems to keep security tighter on.

VI. IDS CHALLENGES

The computing media is starting to use the term IPS (Intrusion Prevention System) more and more, as a replacement for "traditional" IDSs or to make a distinction between them. The IPS is a prevention/protection system for guarding against intrusions, and not just recognizing and reporting them like most IDSs do. There are two main characteristics which distinguish a (network) IDS from a (network) IPS:

1. The IPS sits inline on the IPS network, and does not just passively listen to the network like an IDS (traditionally placed as a sniffer on the network).
2. An IPS has the ability to immediately block intrusions, no matter what transport protocol is used and without reconfiguring a third-party device, which means that the IPS can filter and block packets in native mode (using techniques such as dropping a connection, dropping offending packets, or blocking an intruder).

REFERENCES

[1] Liepins, G. E.; Vaccaro, H. S.: Intrusion Detection: Its role and validation, Computers & Security 11/1992, 347 – 355.
[2] Heberlein, L. T.; Levitt, K. N.; Mukherjee, B.: A method to detect intrusive activity in a networked environment, Proc. of the 14th National Computer Security Conference, Washington D. C., Oct. 1991, 362 – 371.
[3] Proctor, Paul, The Practical Intrusion Detection Handbook, Prentice Hall, 2001.
[4] Shipley, Greg, "Watching the Watchers: Intrusion Detection," Network Computing, November 13, 2000.
[5] http://www.intrusion.com.

AUTHORS

First Author – KANIKA, M.TECH(COMPUTER SCIENCE & ENGNEERING), Email: Kanikagiri@ymail.com
Second Author – URMILA, M.TECH(COMPUTER SCIENCE & ENGNEERING), Email: tajurmila12@gmail.com