INTRUSION PREVENTION SYSTEM

Amjad Abdallah Abdelkarim[1], Hebah H. O. Nasereddin[2]

[1] Mobile Solutions Developer, General Center for Software Development
[2] Computer Information Systems Department. Faculty of Information Systems and Technology, Middle East University, Amman **(JORDAN)**
E-mails: amjad_abdelkarim@hotmail.com, hebah66@hotmail.com

ABSTRACT

New research is going towards find new protection system that offer advanced features that protect computer systems from any attack. This paper describes how intrusion prevention system work, some features that intrusion prevention system have, advantages and disadvantages of intrusion prevention system, some different between intrusion prevention system and intrusion detection system.

Key words: Intrusion Prevention System, Intrusion Detection System, Firewall, IPS.

1. INTRODUCTION

With the explosion in Internet connectivity and the mainstream use of broadband and mobile technologies, there has been a huge increase in the number of computer systems and storage devices connected to the public network. With an ever-increasing reliance on computing infrastructure, we find that our critical IT assets, confidential data and intellectual property are more susceptible to cyber attack than ever before.

In response to the changing threat landscape, Network Intrusion Prevention Systems was developed to provide advanced protection beyond that offered by firewalls and Intrusion Detection Systems. Firewalls and Intrusion Detection Systems provide security but do not arrive the point that Intrusion Prevention System provides.

IPS is a new technology that provides security for computer systems with new features that are effective in facing threats.

Intrusion prevention system (IPS) considered the next step in the evolution of intrusion detection system (IDS). IPS is a software or hardware that has ability to detect attacks whether known or unknown, and prevent attack to complete the needed job successfully. [1]

Also we can define the IPS as a network security device that monitors network and/or system activities for unwanted behavior and can interacts to prevent those activities. [2]

The work of an IPS in a network if often mixed with application-layer firewall. Firewall is a very different type of technology for example firewall use full proxy features to decode and reassemble packets in other hand not all IPS perform full proxy-like processing. [2]

IPS can considered as important component in any IT system defense. There are many reasons that IPS considered like that, among that it protect from denial of service attacks and protect any weakness points in any software. The features of IPS are used in large organizations and the individual users in homes began to use it.

2. IPS IN DETAILS

The need to protect data and networks, and the need to stop attacks and prevent it is the reason that the IPS was found [3]. Firewall act like IPS, but IPS focus on attack prevention at layers that most firewalls are not able to decipher, at least not yet. [1]

There are many types of IPS that practice in many areas, these types are inline network intrusion detection system, application-based firewalls/IDS, layer seven switches, network-based application IDSs, deceptive applications. [1]

IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. As we mentioned before IPS products have ability to implement firewall rules, but it is not a core function of IPS. Also IPS offers deeper watch and monitor into network operations like bad logons, inappropriate content and many other network and application layer functions. [2]

IPS focus on what attack does, its behavior. IPS use signatures and it detect intrusions on the analysis of the traffic. The IPS prevents a large amount of downtime that would occur if it were not there, this is done by it stopping any damage that may have made its way to the databases from internal or even external attacks. The IPS also makes it easier for the administrators to see where attacks are coming from so that they can address them and prevent any further attacks from that location. [3]

An IPS device must use inspection to perform advanced protection against new types of attacks. It performs TCP segment reassembly, traffic analysis, application protocol validation, and signature matching to identify the attack.

IPS is a system that protects the following: [4]

- Confidentiality: that it protect the information that stored on a computer and it prevent unauthorized use of that information (Viewing or Copying).
- Integrity: IPS protects the integrity of information and prevents the alteration on that information from unauthorized users.

- Availability: Protecting the availability of computing resource, network, system or stored information and it prevent any use or access by unauthorized users.

Network IPS solutions (NIPS), designed to protect critical infrastructure by blocking internal and external on the wire and are considered the first line of defense. [4] Host IPS solutions (HIPS) designed to protect critical systems and applications by blocking attacks at the host and are considered the last line of defense. [4]

HIPS can handle encrypted and unencrypted traffic equally, because it can analyze the data after it has been decrypted on the host. NIPS do not use processor and memory on computer hosts but uses its own CPU and memory. NIPS are a single point of failure, which is considered a disadvantage; however, this property also makes it simpler to maintain. However, this attribute applies to all network devices like routers and switches and can be overcome by implementing the network accordingly. NIPS can detect events scattered over the network and can react, whereas with a HIPS, only the host's data itself is available to make a decision. It would take too much time to report it to a central decision making engine and report back to block. [2]

So, when we deploy both network and host IPS technologies they will provides the greatest level of protection for critical data and critical applications.

Wireless intrusion prevention system (WIPS) is to prevent unauthorized network access to local area networks and other information assets by wireless devices [5].

3. IPS ADVANTAGES AND DISADVANTAGES

Like any new development there are advantages and disadvantages in it. One of the most common problems with an IPS is the detection of false positives or false negative, this occurs when the system blocks activity on the network because it is out of the normal and so it assumes it is malicious, causing denial of service to a valid users, trying to do a valid procedure; or in the case of a false negative, allowing a malicious to go by. Considering that this problem found in IDS; however it should be one of the main goals of the network administrators and the manufacturers of IPSs to minimize this as much as they can [3].

Other problem that occurred in IPS that it starts to be quite expensive. Also, if there are multiple IPSs on the network then every packet of data must make multiple stops from its original destination to get to the end user, this will cause loss of network performance and it's another problem. [3]

Even these down sides the benefits of IPs that we receive lead us to protection that any one other security method can provide. One of the IPS advantages that it has ability to act like antivirus software by detecting malicious signatures, stopping them then showing where are they coming from, and where they are trying to go. IPSs can prevent hackers to damage data on a users system or cause on overflow of network traffic. [3]

4. IPS REAL WORLD APPLICATION

Widener University shows a real practice of IPS. The goal of use IPS in Widener University is to protect their database as well as their users on their network; the major difficulty in doing this was their large amount of foreign computers with access onto their network. This meant that they had many students, computers connecting onto their network with already infected and un-patched software. This is a challenge many institutions and corporations also have as they open their networks to mobile workers, students, and other authorized guests. The way which Widener University used a IPS to address this issue was by placing a IPS in front of the firewall for incoming traffic from external sources, and then placing another IPS behind the firewall for outgoing traffic from internal users, accessing their databases. This proved to be very helpful on the Universities network and was able to stop attacks from malicious code. [3]

From the Widener University case we can show that IPS can play a very important rule in network security. Without the use of IPS in Widener University the IT department will face huge problems.

5. COMPARE IPS WITH IDS

IDS may be effective at detecting suspicious activity, but do not provide adequate protection against attacks.

IPS systems have some advantages over intrusion detection systems (IDS). One advantage is they are designed to sit in line with traffic flows and prevent attacks in real-time. In addition, most IPS solutions have the ability to look at (decode) layer 7 protocols like HTTP, FTP, and SMTP which provides greater awareness. However, when deploying network-based IPS (NIPS), consideration should be given to whether the network segment is encrypted since not as many products are able to support inspection of such traffic. [2]

6. CONCLUSION

IPS is very effective technique to protect databases and networks from unauthorized users. It is used in many organizations to keep its own data secure. IPS like any other development, it has some limitations and many advantages.

Combining network and host IPS technology results in the most comprehensive and robust defensive posture. Implementing and deploying proactive IPS technologies will result in fewer successful attacks, more efficient use of security resources, and lower operating costs than simply deploying a single, limited technology and praying you avoid an attack.

Combining IPS, IDS and Firewall technologies will provide a strong defense line to protect systems from

any attack, for example firewall play as first defense line that connect to the second defense line IDS, and first and second lines connect to the third defense line IPS. Combining these three technologies will generate a great protection for any system.

IPS is very useful to use in large networks. We expect to see more real world applications that use IPS in coming days.

REFERENCES

1. Desai, Neil. Intrusion Prevention Systems: the Next Step in the Evolution of IDS. Accessed on January 1, 2010. Available at http://www.securityfocus.com/infocus/1670
2. NIST SP 800-83, Guide to Malware Incident Prevention and Handling. Accessed on January 1, 2010. Available at http://en.wikipedia/wiki/Intrusion_prevention_system.
3. Nick Ierace, Cesar Urrution and Richard Bassett, “Intrusion Prevention System”.
4. “Network Intrusion Prevention Systems Justification and ROI”, MacAfee, INC.3956 Freedom circle, Santa Clara., www.mcafee.com.
5. http://en.wikipedia/wiki/Wireless_Intrusion_prevention_system Accessed on January 1, 2010.