Comparison of network security tools- Firewall, Intrusion Detection System and Honeypot

Tejvir Kaur[1], Vimmi Malhotra[2], Dr. Dheerendra Singh[3]
[123]Department of Computer Science, SUS College of Engineering & Technology, Mohali, India

Abstract: With the advent of Internet, personal computers and computer networks are becoming increasingly vulnerable to various kinds of attacks. Information has become like an asset that needs to be protected from attacks. Due to attack privacy can be violated and important data can be lost. The attacks are usually caused by a failure to implement security policies and failure of using of security tools that are readily available. The various security tools that are available are Firewall, Intrusion Detection System and Honeypot. Each tool has its own features, advantages and disadvantages.

Keywords: Firewall, Honeypot, Intrusion detection system, Network security tools, Security.

Introduction

Intrusion is the act of violating the security policy that pertains to an information system. Intrusion detection can be defined as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations of computer security policies, acceptable use policies or standard security practices. Incidents have many causes such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized [1]. Intrusion detection provides the following functions.

- Monitoring and analysis of user and system activity.
- Auditing of system configurations and vulnerabilities.
- Assessing the integrity of critical system and data files.
- Statistical analysis of activity patterns based on the matching to known attacks.
- Abnormal activity analysis.
- Operating system audit [2].
-

Currently available network security solutions

The number of people connecting to the Internet is increasing very rapidly. The ease of use and the connectivity the Internet provides is highly useful but the risks involved and malicious intrusions are also increasing day by day. Exploitation of computer networks is getting more common. It is completely critical for business organization as well as individuals to protect their data from serious threats that would aim to steal their information. There are many security solutions available in the market. Some of them are like Firewall, Intrusion Detection System (IDS), Honeypot which are explained below.

A. Firewall

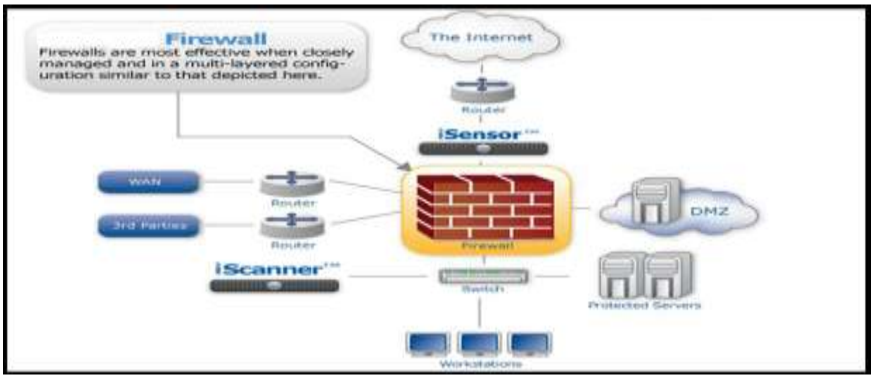
Firewall
Firewalls are most effective when closely managed and in a multi-layered configuration similar to that depicted here.
The Internet
Router
iSensor™
WAN
Router
3rd Parties
Router
Firewall
DMZ
iScanner™
Switch
Protected Servers
Workstations

Figure 1: Firewall [3]

A firewall is a combination of hardware and software that isolates an organization's internal network from other networks, allowing some packets to pass and blocking others. It functions to avoid unauthorized or illegal sessions established to the devices in the network areas it protects. Firewalls are configured to protect against unauthenticated interactive logins from the outside world. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Basically, numbers of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in-depth network security protection. Administrators that manage the firewalls have a have to be careful while setting the firewall rules [4].

Types of Firewall

- **Packet-Filtering Router**

A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is configured to filter packets going in both directions. Filtering rules are based on information contained in a network packet, which include the source IP address, destination IP address, source and destination transport-level address, IP protocol field and interface. The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. The default action can either be to discard or forward the packet.

- **Application level gateways**

An application-level gateway acts as a relay of application-level traffic. It is also known as proxy server. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.

Application-level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level. The main disadvantage of this type of gateway is the additional processing overhead on each connection.

- **Circuit level gateways**

The Circuit level gateway can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection, instead the gateway sets up two TCP connections. One connection is set up between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed [5].

Advantages of Firewalls: Following are the advantages of Firewalls:
i. Firewalls can prevent the traffic which is non-legitimate.
ii. Firewalls can filter those protocols and services that can be easily exploited.
iii. A firewall helps protecting the internal network by hiding names of internal systems from the outside hosts.
iv. Firewalls can concentrate extended logging of network traffic on one system.

Disadvantages of Firewalls: Following are the disadvantages of Firewalls:
i. Firewalls use set of rules that are manually configured to differentiate legitimate traffic from non-legitimate traffic.
ii. The firewall can't react to a network attack nor can initiate effective counter-measures.
iii. Most firewalls do not analyze the contents of the data packets that make up network traffic.
iv. Firewalls cannot prevent attacks coming from Intranet.
v. Filtering rules of the firewall cannot prevent attack coming from application layer [6].

B. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) helps information systems to deal with attacks. This is accomplished by collecting information from a variety of systems and network sources. The information collected is analyzed for possible security problems. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. The intrusions may include attacks both from outside the organization as well as within the organization [7].

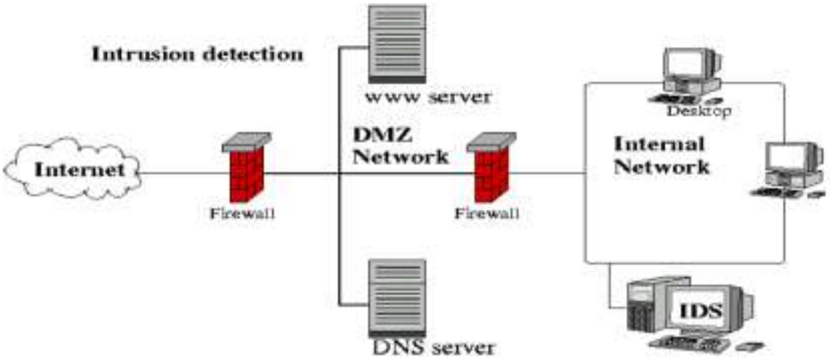

Figure 2: Intrusion detection System [8]

Advantages of IDS:
i) IDS are easier to deploy as it does not affect existing systems or infrastructure.
ii) Network based IDS sensors can detect many attacks by checking the packet headers for any malicious attack like TCP SYN attack, fragmented packet attack etc.
iii) IDS monitor traffic on a real time. So, network based IDS can detect malicious activity as they occur.
iv) IDS sensor deployed outside the firewall can detect malicious attacks on resources behind the firewall [7].

Disadvantages of IDS :
i) IDS is not an alternative to strong user identification and authentication mechanism.
ii) IDS is not a solution to all security concerns.
iii) Human intervention is required to investigate the attack once it is detected and reported.
iv) False positives occur when IDS incorrectly identifies normal activity as being malicious.
v) False negatives occur when IDS fails to detect the malicious activity [7].

C. Honeypot

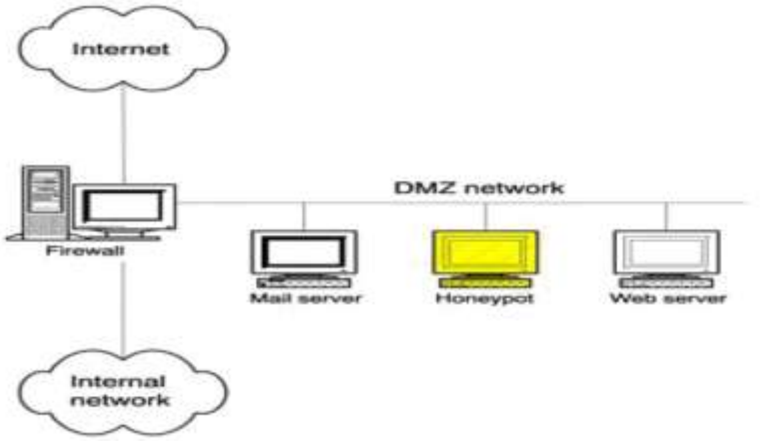

Figure 3: Network Diagram of a production honeypot deployed on a DMZ to detect attacks [9]

A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. A honeypot works by fooling attackers into believing that it is a legitimate system. The attackers attack the system without knowing that they are being observed. When an attacker attempts to compromise a honeypot, its attack-related information, such as the IP address of the attacker, will be collected. This activity done by the attacker provides valuable information and analysis on attacking techniques, allowing system administrators to trace back to the source of attack if required [10]. In general honeypots can be divided into two categories.

Production Honeypots: Production honeypots are used to assist an organization in protecting its internal IT infrastructure. These secure the organization by policing its IT environment to identify attacks. These honeypots are useful in catching hackers with criminal intentions. The implementation and deployment of these honeypots are relatively easier than research honeypots because these have less purpose and require fewer functions. As a result, they also provide less evidence about hacker’s attack patterns and motives**.**

Research Honeypots: Research honeypots are complex. They are designed to collect as much information as possible about the hackers and their activities. Their primary mission is to research the threats organization may face, such as who the attackers are, how they are organized, what kind of tools they use to attack other systems, and where they obtained those tools. While production honeypots are like the police, research honeypots act as their intelligence counterpart and their mission is to collect information about the attacker. The information gathered by research honeypots will help the organization to better understand the hackers attack patterns, motives and how they function [9].

Advantages of Honeypot:

1. Small Data Sets: Honeypots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day with traditional technologies will only log a hundred alerts with honeypots. This makes the data honeypots collect much higher value, easier to manage and simpler to analyze.

2. **Reduced False Positives:** One of the greatest challenges with most detection technologies is the generation of false positives or false alerts. It's similar to the story of the 'boy who cried wolf'. The larger the probability that a security technology produces a false positive the less likely the technology will be deployed. Honeypots dramatically reduce false positives. Any activity with honeypots is by definition unauthorized, making it extremely efficient at detecting attacks.

3. **Catching False Negatives:** Another challenge of traditional technologies is failing to detect unknown attacks. This is a critical difference between honeypots and traditional computer security technologies which rely upon known signatures or upon statistical detection. Signature-based security technologies by definition imply that "someone is going to get hurt" before the new attack is discovered and a signature is distributed. Statistical detection also suffers from probabilistic failures – there is some non-zero probability that a new kind of attack is going to go undetected. Honeypots on the other hand can easily identify and capture new attacks against them. Any activity with the Honeypot is an anomaly, making new or unseen attacks easily stand out.

4. **Encryption:** It does not matter if an attack or malicious activity is encrypted, the Honeypot will capture the activity. As more and more organizations adopt encryption within their environments (such as SSH, IPSec, and SSL) this becomes a major issue. Honeypots can do this because the encrypted probes and attacks interact with the Honeypot as an end point, where the activity is decrypted by the Honeypot.

5. **IPv6:** Honeypots work in any IP environment, regardless of the IP protocol, including IPv6. IPv6 is the new IP standard that many organizations, such as the Department of Defense, and many countries, such as Japan, are actively adopting. Many current technologies, such as firewalls or IDS sensors, cannot handle IPv6.

6. **Highly Flexible:** Honeypots are extremely adaptable, with the ability to be used in a variety of environments, everything from a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.

7. **Minimal Resources**: Honeypots require minimal resources, even on the largest of networks. A simple, aging Pentium computer can monitor literally millions of IP addresses [11].

Disadvantages of Honeypots:
Apart from all the advantages, honeypots also have some disadvantages. Disadvantages of honeypots are listed below:

1. **Risk:** Honeypots are a security resource the bad guys to interact with, there is a risk that an attacker could use a honeypot to attack or harm other non-honeypot systems. This risk varies with the type of honeypot used. For example, simple honeypot such as KFSensor has very little risk. Honeynets, a more complex solution, have a great deal of risk [12]. The risk levels are variable for different kinds of honeypot deployments. The usual rule is that the more complicated the deception, the greater the risk. Honeypots that are high-interaction such as Gen I Honeynets are inherently more risky because there is an actual computer involved.

2. **Limited Field of View:** Honeypots only see or capture that which interacts with them. They are not a passive device that captures activity to all other systems. Instead, they only have value when directly interacted with. In many ways honeypots are like a microscope. They have a limited field of view, but a field of view that gives them great detail of information.

3. **Discovery and Fingerprinting:** Though risk of discovery of a honeypot is small for script kiddies and worms, there is always a chance that advanced blackhats would be able to discover the honeypot [13]. A simple mistake in the

deception is all a savvy attacker needs to “fingerprint” the honeypot. This could be a misspelled word in one service emulation or even a suspicious looking content in the honeypot. The hacker would be able to flag the honeypot as “dangerous” and in his next attacks; he would most certainly bypass the honeypot. In fact, armed with the knowledge, an advanced blackhat could even spoof attacks to the honeypot thus redirecting attention while he attacks other vulnerable systems in the network [14].

Comparison between Honeypots, Firewalls and IDS

A comparison is made between Honeypots, Firewalls and IDS in the following section.

Honeypots vs Firewalls

A firewall is designed to keep the attackers out of the network whereas honeypots are designed to entice the hackers to attack the system. This is done so that a security researcher can know how hackers operate and can know which systems and ports the hackers are most interested in. Also firewalls log activities and logs also contains events related to production systems. However in case of honeypot, the logs are only due to non-productive systems, these are the systems that no one should be interacting with. So a firewall log contains 1000 entries of all the systems of the network whereas the honeypot’s log only contain 5-10 entries.

Honeypots vs IDS

NIDS also suffer from high false positive rates. The value of a honeypot is determined by the information that can be obtained from it. Monitoring the data that enters and leaves a honeypot lets us gather information that is not available to NIDS. To detect malicious behavior, NIDS require signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerabilities that are not yet understood. Consequently, forensic analysis of data collected from honeypots is less likely to lead to false positives than data collected by NIDS.IDS is used as an alternative for building a shield around the network. The shielding approach is deficient in several ways, including failure to prevent attacks from insiders. IDS often depend upon signature matching or statistical models to identify attacks. This means that unknown or novel threats may not be detected. In contrast, honeypots are designed to capture all known and unknown attacks directed against them. Because any network activity related to the honeypot represents an anomaly, even the stealthiest activity will register on a honeypot [15].

References

[1]. K. Scarfone and P. Mell, ”Guide to Intrusion Detection and Prevention Systems (IDPS),” Gaithersburg, MD, Rep. NIST Special Publication 800-94,Feb. 2007.

[2]. D. Rozenblum, “Understanding Intrusion Detection System,” www.sans.org/reading_room/whitepapers/detection/understanding-intrusiondetection-systems_337, October 31, 2003.

[3]. S. Nassar, A.E. Sayed, N. Aiad, “Improve the Network Performance By using Parallel Firewalls,” in Proc. of 6th International Conference on Networked Computing, May 2010, pp. 1-5.

[4]. S. Ioannidis et al., “Implementing a Distributed Firewall,” in Proceedings of the ACM Computer and Communication Security (CCS), pp. 190-199, 2000.

[5]. W. Stallings, Cryptography and Network Security Principles and Practices. 4th ed.,Prentice Hall, 2005.

[6]. X. Jhang, C. Li, W. Zheng, “Intrusion Prevention System Design.” in Proc. of 4th International Conference on Computer and Information Technology, pp. 386-390, Sept. 2004.

[7]. A. Samrah, “Intrusion Detection Systems; Definition, Need and Challenges,” http://www.sans.org/reading_room/whitepapers/detection/intrusion-detectionsystems-definition-challenges_343, October 31, 2003.

[8]. Harek Haugerud, “Intrusion detection and firewall security,” Available: http://www.iu.hio.no/teaching/materials/MS004A/html/pictures/ids.png.

[9]. Levin, J. and Labella, R., “The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks”, IEEE Proceedings, pp.92-99, 18 June 2003.

[10]. “Honeypot Security”, http://www.infosec.gov.hk/english/technical/files/honeypots.pdf.

[11]. Ryan Talabis,” Honeypots 101: What’s in it for me?” http://www.philippinehoneynet.org/, Fetched 21/06/2011.

[12]. Tang, X. "The Generation of Attack Signatures Based on Virtual Honeypots”, International Conference on Parallel and Distributed Computing, Applications and Technologies, 2010, pp.435-439.

[13]. “Snort”, http://www.snort.org/assets/166/snort_manual.pdf.

[14]. John E. Canavan,” Fundamentals of Network Security”, http://www.artechhouse.com.

[15]. Provos, N., “A Virtual Honeypot Framework”, SSYM’04 Proceedings of the 13th conference on USENIX Security Symposium, Volume 13, 2004.