Identification Security at Unauthorized Use of Information System

Navpreet Kaur and Dhawaleswar Rao,

Lovely Professional University, Phagwara, Punjab, ndia

Summary
Security is the primary requirement in this era of informationization. Threats and worms are rising with a high degree and penetrating into the system, there is a need of such a security system that should analyze and provide valuable information to the organization. Honeypot provides a technology that adds a layer to the network security and the goal of honeypot is to distract the attacker from real systems and to gain valuable information about them. In comparison to other intrusion detection technologies, Honeypot is far better because it has the ability to detect new attacks and improve the security of the network by using the existing intelligence of the security technologies. Honeypot is designed to get compromised with the new threats and welcome the attackers to attack and analyze their behavior. So, Honeypot is an attractive alternative as it acts as trap to detect the suspicious that breaches the network security.

Key words:
Network Security, Honeypots, Firewall, Intrusion analysis, Attacks.

1. Introduction

Security can provide control to system. It can reduce the risk but cannot eliminate the risk completely. The security of information system starts from the physical level of security. Physical security means providing protection or restricting unauthorized access from physically accessing the resources and stored information. It includes protecting equipment s from damage or loss. The second layer of network security architecture is the system security that means the administrator provides limited access of information to users or individuals by views or groups.
The next very important layer is network security layer of network security architecture. This layer plays a very crucial role because every organization has some information that someone else want. So security is to be required in today's world over the network when everything is surrounded by the internet and there is a vast communication and acute data and files are transferred within a few minutes. A network is a system of interconnected computers and network security is restricting invaders access to it.

Manuscript received January 5, 2016
Manuscript revised January 20, 2016

As, the probability of get compromised from the attack is very high and the risk of being attacked is also very high , no matter how hard we try, we can't completely rule out the problem of threats. As there are various security mechanisms or techniques available that provides protection to the organization, but still the risk of being attacked is very high. Honeypot technology act as add on flavor to the existing technologies and is better in terms of detecting the new attacks and gathering the information about the intruder's behavior. We can use anti-virus software but a new type of threat would be there at our doorstep tomorrow. We need a system that detects and checks all the time for new types of threats.

2. Security Identification

2.1 Why Network Security?

Security is a serious issue to be considered. In the past, intruders would periodically attack an organization. Today attacks are nonstop. The attackers are continual, and if an organization lets their guard down for any period of time, the chance of a compromise is very high. The network security is needed because some of the following reasons:
1. *System Automation*: In computer definition automation means a system that reduces the human work or the operation performed by humans manually now replaced by computer procedures System security automation is urgent issue and is the critical one. Automation system security uses the technology to protect system from virus, spam, threats, attacks etc.

2. *Blackhats*: These are computer criminals who tried to steal information from network. They violate the communication traffic over the network. Black hat attackers illegally break the system security. They are better known as "CRACKERS".

3. *Worms, Trojan, and DOS attack*: Now a day's internet usage in people's everyday life is so acute that till from the morning to evening, everyone got stuck in the internet web. The usage of internet is so easy too with the danger of cyber threats and attacks. So there is a need to better

prepare ourselves and our computer systems from the cyber threats like worms, Trojans and various DOS attacks.

2.2 Security Models

There are various security mechanisms or techniques available that provides protection to the organization. These security mechanisms developed to be used in the network architecture follows any of the security models. An architecture that provides security over the five layers of network include physical security, system security, network security, application security, management security follows the following security models:

1. PDR-Protection, Detection, Reaction.
2. P2DR- Policy, Protection, Detection & Reaction.
3. PDRR-Policy, Protection, Detection, Reaction & Restore.

3. Intrusion Detection System

The detection system uses the mechanism or technology that is used to gather intruder's information as well as track the path through which the intruder penetrate into the system by breaching the security layer of the organization. Although the intrusion detection systems are available for detecting intruders but intruders try to breach security with another new way every time.

Intrusion detection System can be a hardware device or a software application, its job is to monitor the traffic over the network and other malicious operations. This intrusion detection system may act as an alert alarm for the organization and also for the system administrator. It prevents the system from the harmful activities by analyzing and detecting the threats and give response to the system.

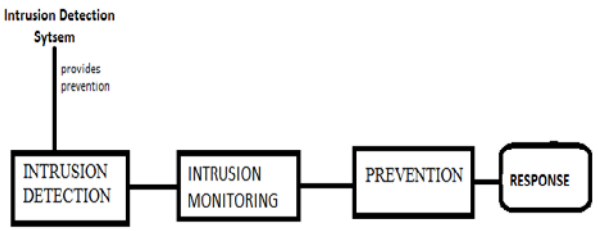

Fig. 1 Intrusion Detection System

3.1 Types of Intrusion Detection System

1. Network Intrusion Detection System (NIDS)

The NIDS detect the threats inside the network and are placed within the network. The NIDS analysis and monitors the traffic of packets within the network and scan the packets and respond upon detection of any threat.

2. Host Intrusion Detection System (HIDS)

Host Intrusion detection system are run on the individual computers or hosts on the network. This intrusion detection system scans the outgoing or incoming packets from the computers or individual devices and alerts the users or the system administrators.

3. Signature Based Intrusion Detection System

A signature based IDS collects the packets and compares it with the large database. Thus this system detects the attack that had already been documented in from the past behavior.

4. Anomaly Based Intrusion Detection System

The system administrator defines a fixed baseline and this baseline will be used to detect anomalies from the normal behavior of the traffic. This alerts the user and the administrator when the anomalous traffic is detected.

3.2 Limitations of Intrusion detection System

1. *Could Not Detect Encrypted Data:* Intrusion detection system is not able to detect encrypted packets and allows them to enter the network that may be an attack to the software.
2. *False Positive And False Negative:* Although intrusion detection system detects attackers or intruders most of the times but are not perfect it fails, because of the two reasons first it create false alarms when actually no attack is there (known as false positive) and does not create an alarm for real attack (known as false negative).So these false detect ions causes the abnormal behavior in the network.
3. In signature intrusion detection system it is difficult to monitor and analyze large amount of data.

3.3 New threats and attacks

Threats and attacks are penetrating with a high magnitude in spite of having various security mechanisms. Just by having anti-virus software; it is very difficult to say that the systems are free from viruses, risks and worms. Same as sitting behind a firewall doesn't means that the network is out of reach of malicious activities and intents of the intruders. This is all because every new virus or new attack finds some different way to break through the security infrastructure, which often goes undetected by the security technologies in place. So improving security is the issue, which is in more concern against the increasing rate of threat to the organization. Although the intrusion detection system is providing security to the network from various attacks and threats but still there is a new attack at the doorstep. Some of the new threats and attacks that are endangering the organizational security are as follows:

a. *Phishing:* Phishing means acquiring credentials details like usernames and passwords by claiming as a genuine user. It's an attempt to gather private information. Most commonly used phishing is email spoofing, in which user is directed to a website where they are asked to enter personnel information like user name, passwords, credit card numbers etc.

b. *Botnets:* A collection of compromised systems that communicates through an internet connected programs know as a botnet and referred to as "ZOMBIES". Intruder distributes the virus through software that can turn your computer to a bot .This network of botnets is used to send spam emails, virus, worms.

c. *Trojan and worms:* Trojan and worms are the malicious files that cause damage to the computer programs. Trojan and worms can delete important files from the system or sometimes may lead to crash of hard drive. Trojan may contain some malicious code when the link is opened, it triggers and cause damage for example: some email attachment. Trojan and worms causes damage not to the hardware components but it causes damage to the software programs.

d. *Impersonation:* impersonation is the ability to pretend to be someone else or some other process to gain access over the network and commit some fraud. Impersonators gather information about the organization by eavesdropping or by email phishing and violate the security of the organization.

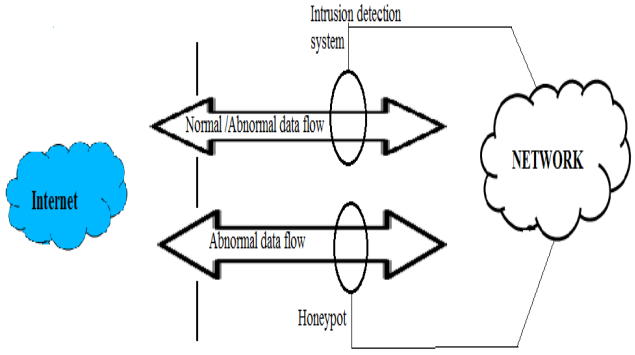

Fig. 2 Abnormal behavior of traffic in the network

4. HONEYPOT: A new approach to security

Honey pot is an additional layer to security. Honeypot is an information system that captures the data and information of the attacker. Honeypot is a device or a tactic to identify an illegal attempt or some intrusion. The Honeypot may consist of the following:

- A computer
- Data
- A network site

So Honeypot technology is used to detect the attack and observe the intruders behavior, so that this information is used to improve security. It is used as a trap to capture the intruders who penetrates into the network without any authorizes access.

4.1 Classification of honeypot

a. Classification based on implementation:

1. *Server Side Honeypots:* Server based honeypot is based on traditional honeypot technology. These honeypots are inactively waits until it was attacked.
2. *Client side honeypots:* Client honeypots actively participate to detect an attack, it interacts with the server and find out the attack.

b. Classification based on interaction:

1. *Low Interaction Honeypots*

- Low interaction honeypot has limited services.
- Low interaction Honeypot follow the services that are commonly provided by the attacker.
- They use few resources and easy to install.
- But the limitation is that it captures only limited information of the legitimate user.
- Example: honeyd.

2. *High Interactive Honeypots*

- High interaction honeypots provides a lot of services, real services.
- They provide services to the attacker so that he can waste lots of his time by organizing various virtual machines on a single physical machine.
- High interaction honeypots are very complex because they involve real operating system and applications.
- It provides with clear detailed information of the attackers method.
- Even in the worst condition it is not possible that the attacker cross over the high interaction Honeypot, it is used as way to attack the network.
- Example: honeynet.

3. *Pure Honeypots:* These are the systems using them the actions of the intruder are monitored by the casual tapes, which are installed on the honeypot's link in the network.

4.2 How Honeypot works?

The Honeypot technology is used to monitor the network where every packet entering or leaving is captured and analyzed. It includes:

- Data control
- Data capture
- Data analysis

Data Control: The intrusion detection system captures and analysis the intruders attack behavior, so the activity log of the intruder is captured. For being on a safer side, data captured after the Honeypot is attacked, the attacker tries to spur the activity log. So the Honeypot system restricts the outflow of the data once it is captured. Honeypot only allows the permission to enter into the network but the external way is blocked. On the other side it directs the attackers address to some new host that appears as useful information.

Data Capture: Data capture technology captures the attack behavior of the intruder. It captures the intruder behavior activity log without noticing the attacker. By analysis the log the attack method can be found out.

Data Analysis: Data analysis is done on the activity log to find out some new attack or the attack method. Data analysis includes the network protocol analysis, network behavior analysis, analysis of attack characteristics .The main purpose of data analysis is to check some abnormal traffic behavior, if such type of warning is there it warns the system and protects it from the attack.

4.3 Research Methodology

As there are various security mechanisms or techniques available that provides protection to the organization, but still the risk of being attacked is very high. So honeypot is a new technology that not only provides prevention but have the ability to get compromised to capture the suspicious agents. The honeypot composed of the three modules basically data control block, data capture block and then analysis of data to capture the intruder behavior and attack type and then generate the response for that particular malicious activity.

i. The main goal of the bot or suspicious agent is to enter into the network by breaking the security layer of the organization, the main entry point is through the internet. The intruder can harm the organization's data or information by sending the packets and suspicious data through the internet that may corrupt the organization's information.
ii. The data control block of the honeypot captures the network flow and communication between the intruder and the server.
iii. The next when the intruder enters into the network and gets detected by the security technique, the data capture block of the honeypot technology captures the data and generate the log files and create the spam database for further analysis.
iv. If the captures data supposed to be from the suspicious agent or site then it is redirected to honeypot server and if not the forwarded to the destination server for final processing of the request and normal transmission continues.
v. The honeypot server has the log files that are used for the analysis. It will check for the duplicate IP's by analysis from the log created and generate the alerts that will act as an early warning to the network.
vi. The response block is responsible for responding to the system. The spams suspected are redirected to the honeypot server for the gathering of information related to the intruder behavior or if any new type of attack. Then the suspicious packets are blocked by the honeypot.
vii. Honeypot technology concept is very effective in detection of threats. Hence it must be included into organization architecture of the network.

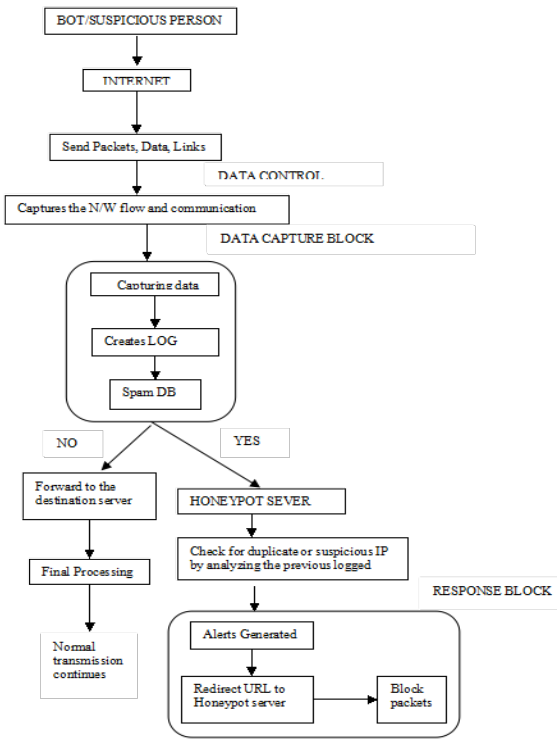

Fig. 3 Honeypot technology flowchart

5. Conclusion

The major goal of honeypot technology is gathering intruder's information as well as track the path through which the intruder penetrate into the system by breaching the security layer of the organization. The conclusion is that, there is a need for tight supervision as well as analysis to predict the future harm to the important information. At the end honeypot is a tool and all security mechanisms have some risk. The risk of using honeypot is that if they are taken by some intruder we can also call him as "CRACKER", and then he may harm the other systems also. As the honeypot is just a tool, so how one can use it, deploy it, it's up to them.

Acknowledgments

I would like to take this opportunity to express my deep sense of gratitude to all who helped me directly or indirectly during this work. The encouragement and critics are sources of innovative ideas, inspiration and cause behind the successful completion of this research paper. I am highly obliged to all faculty members of computer science and engineering department for their support and encouragement. I would like to express my sincere appreciation and gratitude towards my friends for their encouragement, consistent support and invaluable suggestions at the time I needed the most.

References

[1] A. Nisha H, "Campus security using honeypot," in CEEE, pp. 153–156, 2013.
[2] T. Kaur, V. Malhotra, and Dr. D. Singh, "Comparison of network security tools-Firewall, Intrusion detection system and Honeypot," in ISSN, vol. 3., pp. 200-204, February 2014.
[3] L.Spitzer, "Honeypots: Catching the insider threat," vol. NA, pp. 1-10,2003
[4] E. Peter, and T. Schiller, "A practical guide to honeypots,"15 April 2008. [Online]. Available: http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html.[Accessed 1 September 2014].
[5] A. Verma, "Production Honeypots: An Organization's view," SANS, vol. NA, no. NA, p. 1-30, 2003.
[6] R. Koch, M. Golling, and G. Dareo, "Attracting sophisticated attacks to secure systems: A new honeypot architecture," IEEE, vol. NA, pp. 409-410, 2013.
[7] X. Suo, X. Hue, and Y. Gao, "Research on the application of honeypot technology in intrusion detection system," IEEE, vol. NA, pp. 1030- 1032, 2014.

Navpreet kaur received the B.Tech in Computer Science Engineering from Malout Institute of Management and Information Technology in 2013 and pursuing M.Tech. in Computer Science and Engineering from Lovely professional University.