International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 107-109
Published Online December - January 2016 in IJEAST (http://www.ijeast.com)

INTRUDER DETECTION SYSTEM

Gayatri Bhagat
G.L.B.I.T.M

Megha Soni
G.L.B.I.T.M

Priyanka Singh
G.L.B.I.T.M

ABSTRACT - A computer-implemented intruder detection system and method that monitors a computer system in real-time for activity indicative of attempted or actual access by unauthorized persons or computers. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile, detects events that indicate an unauthorized entry into the computer system, notifies a control function about the unauthorized users and events that indicate unauthorized entry into the computer system and has a control function that automatically takes action in response to the event. The user profiles are dynamically constructed for each computer user when the computer user first attempts to log into the computer system and upon subsequent logins, the user's profile is dynamically updated. By comparing user behavior to the dynamically built user profile, false alarms are reduced. The system hence provides us with the credentials of the attacker and also notifies us if the Mac address if the person is changed.

I. INTRODUCTION

With the emergence of the Internet as a medium for wide-scale exchanges of sensitive information and financial transactions, maintaining the security and integrity of information is very important. Cyber risk is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy. It's not surprising that governments and businesses around the world are searching for better cyber defense strategies. So basically this paper is an initiative in contributing a bit to the computer security using the concept of Honeypot which is a deception trap, designed to entice an attacker into attempting to compromise the information systems in an organization.

Intruder Detection System works by fooling attackers into believing it is a legitimate system; they attack the system without knowing that they are being observed covertly. When an attacker attempts to compromise a honeypot, attack-related information, such as the IP address and Mac 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.

Honeypots can be used for production or research purposes. They help to protect a network and systems against attacks generated by automated tools used to randomly look for and take over vulnerable systems.

II. HONEYPOT

In the past several years there has been extensive research into honeypot technologies, primarily for detection and information gathering against external threats. This project discusses how honeypot technologies can be used to detect, identify and gather information on the specific threats.

Honeypots are a powerful, new technology with incredible potential. They can do everything from detecting new attacks never seen in the wild before, to tracking automated credit card fraud and identity theft. In the past several years we have seen the technology rapidly develop, with new concepts such as honeypot farms, commercial and open source solutions, and documented findings released. However a great deal of research has been focused on identifying, capturing, and researching external threats. While malicious and dangerous, these attacks are often random with attackers more interested in how many systems they can break into then which systems they break into. This trusted individual knows your networks and organization. Often, these individuals are not after computers, but specific information. This is a risk that has proven far more dangerous, and far more difficult to mitigate.

This paper attempts to discuss how honeypots, an emerging technology, can be incorporated in the Intruder detection system to trace the attacker without his knowledge. A honeypot is a unique security resource. It is something you want the bad guys to interact with. The definition of a honeypot as, defined by the honeypot maillist "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource". What this definition means is honeypots derive their value from threats using them. If the enemy does not interact or use the honeypot, then it has little value. This is very different from most security mechanisms. For example, the last thing you want an attacker to do is interact with your firewall, IDS sensor, or PKI certificate authority. Honeypots are very different, and it is this difference that makes them such a powerful tool in your arsenal.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 107-109
Published Online December - January 2016 in IJEAST (http://www.ijeast.com)

First, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that has many applications to security. They can be used everything from slowing down or stopping automated attacks, capturing new exploits to gathering intelligence on emerging threats or early warning and prediction.
Second, honeypots come in many different shapes and sizes. They can be everything from a Windows program that emulates common services, such as the Windows honeypot KFSensor. In fact, honeypots don't even have to be a computer, instead they can be a credit card number, Excel spread sheet or login and password (commonly called honeytokens).
Apart from these, honeypots have other advantages also. These are:

2.1. 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 hundred alerts with honeypots. This makes the data honeypots collect much higher value, easier to manage and simpler to analyze

2.2. 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.

2.3. 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.

2.4. 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.

- **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.

- **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.

- **Minimal Resources**

Honeypots require minimal resources, even on the largest of networks. A simple, aging Pentium computer can monitor literally millions of IP addresses.
There are two key types of honeypots that play a role:-

1. Honeynets

Honeynets are one of the most advanced and complex honeypots, their primary purposes is to capture extensive information on threats, both internal and external. Honeynets have this flexibility because they are not a standardized solution, instead a Honeynet is a specialized architecture that creates a fishbowl, you can then place any targets systems you want within this fishbowl. Just like a fishbowl, you can create your own virtual world, however instead of adding coral and sand, you add Solaris database servers or Cisco routers. Just like a fishbowl, you can watch everything that is going on, however with a Honeynet the attacker never realizes you are watching them (similar to a one way mirror).

2. Honeytokens

Honeytokens represent one of the newest and most interesting implementations of a honeypot. First, they are not a computer; instead they are a digital entity, such as an Excel spreadsheet. Even though they are not a computer, they share the same definition and concept of honeypot, no one should be interacting with them. An interaction with a honeytoken implies unauthorized or malicious activity. Second, they are extremely flexible; they have the ability to adapt to any environment. The reason for this is simple a honeytoken can pretty much be anything you want. Examples can include a Word document, login and password, database record, or social security number.

III. METHODOLOGY

Motive is basically to adapt a strategy such that intruder unknowingly passes its information rather than gathering from the so called vulnerable system, which itself is prepared to attack the incoming intruder and extract out the methodologies and technologies used by intruder to attack the system, so that security breaches and challenges can be amended and modified to the zenith level of excellence.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 107-109
Published Online December - January 2016 in IJEAST (http://www.ijeast.com)

This kind of system may lead to two conditions for the intruder where either information is extracted from the intruder (level 0) and still unaware or information is extracted and the intruder is further blocked (level 1). Two walled gateway plays the crucial role for defining the intruder to be categorized for level 0 or level 1.
Level 1 Intruders are basically those intruders who will break the 2 walled secure gateways and try to enter in the system. Level 0 Intruders are the ones who are trying to access the system with their tricks and methods would be entertained by the system.
The bait for intruder would be the confidential data, however will be rerouted to the dummy section where the intruder will never be able to reach to such confidential data which actually never existed there and was just an illusion to attract the intruder.

Tools Used

TraceMac- *It is a Windows/Linux command line tool that allows you to trace a specific MAC address through Cisco switches. It works by connecting to a switch using SSH, SNMP, Telnet, HTTP or HTTPS and do some "show commands" and later process in the output, this happens recursively until it finds the switch where that MAC address is directly connected.*

CGX Solution- *The CGX solution monitors device access requests across wired and wireless networks. Besides capturing the MAC addresses of each device, it also collects profiling information such as operating system, device platform, location, time and even user name if possible. Based on this collected information, the CGX can then assign the appropriate access rights to the device, from providing full access, limited access or even restricting access tto effectively "quarantining" devices.*

3.1.3 Wireshark - *Wireshark is the world's most popular network protocol analyzer. It has a rich and powerful feature set and runs on most computing platforms including Windows,*

OS X, Linux, and UNIX. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark has sophisticated wireless protocol analysis support to help administrators troubleshoot wireless networks. With the appropriate driver support, Wireshark can capture traffic "from the air" and decode it into a format that helps administrators track down issues that are causing poor performance, intermittent connectivity, and other common problems.
And thus by tracing the IP address and permanent credentials of the intruder we trace out the current location of the intruder.

IV. CONCLUSION

Cyber security is one of the most urgent issues of the day. Computer networks have always been the target of criminals, and it is likely that the danger of cyber security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations can take to minimize losses from those who seek to do harm.
With the right level of preparation and specialist external assistance, it is possible to control damages, and recover from a cyber breach and its consequences by implementing the Intruder Detection System. We sought to enhance the Intrusion Detection System capability by putting the functionality of the dummy environment into execution.
Intruder Detection System traps the intruder by tracing its credentials. The dummy environment created helps to keep the original system environment secure and hence securing the system's crucial data, it contributes towards the information security of the system.

V. REFERENCES

1.http://www.acsa-admin.org/2003/papers/spitzner.pdf
2.http://www.honeynet.org/papers/profiles/cc-fraud.pdf
3.http://www.honeynet.org/scans/scan28/
4. http://www.tracking-hackers.com/papers/gatechhoneynet.pdf