International Journal For Technological Research In Engineering
Volume 2, Issue 8, April-2015 *ISSN (Online): 2347 - 4718*

ADVANCE TECHNIQUE FOR IP MONITORING

[1]Umar Zia, [2]Mr. Amit Asthana
[1]PG Scholar, [2]Assistant Professor
[1]M.Tech (CSE)
Subharti Institute of Technology and Engineering, Swami Vivekanand Subharti University, Meerut

Abstract: In computer terminology, a honey pot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honey pot 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. This is similar to the police baiting a criminal and then conducting undercover surveillance. two or more honey pots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot" A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated."
Keywords : honeypot, intrusion, honeynet

I. INTRODUCTION

In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. There is also a system monitor tool in my project through which the network administrator monitor and analyze data connected from local area network. RMON is a part of management information base. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Thus the main purpose of this seminar is to explain Audio Steganography and algorithms commonly employed for Audio Steganography and its applications. Remote network monitoring system is also known as RMON.RMON was developed to help network administrator monitor and analyze data connected from local area network. RMON is a part of management information base

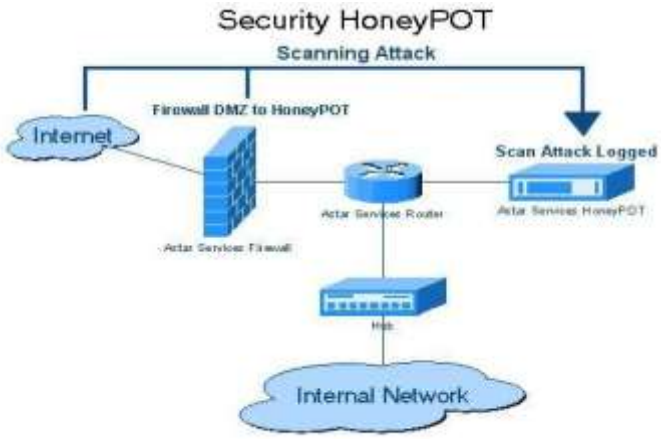
II. HONEYPOTS

An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out.

By luring a hacker into a system, a honeypot serves several purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

Fig 1 Honeypot



III. OBJECTIVES

Hybrid architecture that combines the best features of honeypots and anomaly detection. Hybrid honeypot is the combination of low and high interaction honeypots. We use a variety of anomaly detectors to monitor all traffic to a protected network or service. Attacks against the honeypot are caught, and any incurred state changes are discarded and the alarm is raised. The outcome of processing a request is used to filter future attack instances and could be used to update the anomaly detector. It consists of log having three list of database-

- First (Activelist)-It contains the list of IP blocks from the database and generate the output scheme.
- Second (Blockelist)-It consist of IP addresses which should never be added (either you own them or because they belong to somebody whom you trust a lot). System monitoring tool is very essential for a administrator to have a close look on the activities of his clients.

IV. LITRATURE SURVEY

Honeypots provide a system that can lure the attackers and hackers and response to various security frameworks to control the globe and its environment and network assuming initiative and enterprise security scheme strategies. The proposed model has more advantages that can response accurately and swiftly to unknown attacks and lifetime safer for the network security examine and analysis network activities. We try to employ and develop a honeypot framework to propose a hybrid approach that improves the current security. Steganography literally means secret writing. The technique has been used in various forms for 2500 years or long. It has found its application in various fields including military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. The paper describes the concept of finding natural relationship between a digital cover and a message. The relationship can be used to hide the information in cover without actually replacing or distorting any useful bits of the cover. It introduces a concept called sustainable embedding of message in a cover using natural relationship and representing it using graph theoretic approach. Because of the drawbacks associated with both formal, direct physical observation of research participants and videotaping participants, video screen capture technology is chosen as a better way to track human-computer interaction. Video screen capture technology is an inexpensive, user-friendly way to enhance electronic resource usability studies in any library. Research files can be easily exported into coding software for data analysis. The paper examines a new, non-invasive way to capture student research behavior. It shows how any library could use this same technology to conduct research on how their resources are being used by their user population.

V. RESEARCH METHODOLOGY

In context to intrusion detection following data mining techniques are widely used:-

- Association rules – defines the normal activity by determining attribute correlation or relationships among items in dataset which makes discovery of anomalies becomes easy.
- Frequent Episode rules – describes the audit data relationship using the occurrence of the data.
- Classification – classifies the data into one of the available categories of data as either normal data or one of the types of attacks.
- Clustering – clusters the data into groups with the property of inter-group similarity and intra-group dissimilarity.
- Characterization – differentiates the data, further used for deviation analysis

VI. STEGNOGRAPHY MODULE

A. Encryption

Encryption includes a message or a file encrypting. Encryption involves converting the message to be hidden into a cipher text. Encryption can be done by passing a secret key. Secret key can be used for encryption of the message to be hidden. It provides security by converting it into a cipher text, which will be difficult for hackers to decrypt. Moreover if the message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message.

B. Hide Message

Hiding message is the most important module of steganography. It involves embedding the message into the cover text. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these values often range from 0-255.In order to hide the message, data is first converted into byte format and stored in a byte array. The message is then encrypted and then embed each bits into the LSB position of each pixel position. The least significant (rightmost) bit of each 8-bit byte has been co-opted to hide a text message.

C. Retrieve Message

It involves retrieving the embed message from the file independent of the file format. Once the message has been retrieved it has to be converted into original message or file. This can be done by reading the embedded data from the master file. The read data will be in the bytes format. This message has to be converted into the suitable output file format.

D. Decryption

Decryption includes a message or a file decrypting. Decryption involves converting the cipher text into decrypted format. Decryption can be done by passing a secret key. Secret key can be used for decryption of the message that is hidden. It provides security by converting the cipher text, into the original data message or file. Moreover if the message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message

VII. PLANNING WORK

A. Data Gathering: Data is collected over here for detection of intrusion. Data is collected by packet monitoring system. First I traced the packets captured and built some protocols and was able to display them in my test program. And then (after getting the source code of it), I used the source code to learn the protocol structures. Now my program supports over

15 protocols. My aim is to add all protocols to my program and to make it available to all. Packet capturing (or packet sniffing) is the process of collecting all packets of data that pass through a given network interface. Capturing network packets in our applications is a powerful capability which lets us write network monitoring, packet analyzers and security tools.

B. High Interaction/Low interaction Honeypot:- In this data is divided on the basis on known and unknown attack. Known attacks are send to high interaction honeypot and unknown attacks are send to low interaction honeypot. Honeypot is a network security tool written to observe attacks against network services. as a low-interactive honeypot, it collects information regarding known or unknown network-based attacks and uses plug-in for automated analysis.

C. Anomaly Detection and Neural network:- In this phase anomaly and neural network detection techniques are applied here for detecting intrusions.

D. Analyzing: - Data in analyzed here and then it send it to the log.

E. Processing Data: - In this data is processed as compared with that stored in backend (database).

F. Log: - It is database which consists of three tables.

First (Active list)-It contains the list of IP blocks from the database and generate the output scheme. Second (Blocklist)-It consist of IP addresses which should never be added (either you own them or because they belong to somebody whom you trust a lot). Third (Controllist)-It holds the last time when the data was updated

G. Alarm: - If honeypot detects an intrusion then it raises the alarm.

VIII. CONCLUSION

In a LAN network, each client is identified by its own IP address. In the client-server model, we can use remote network monitoring systems. The server part waits for client's connection and for each newly connected client. The client side, its core function is sending a screen shot of the client's desktop when administrator wants to monitor client system. It has one more feature you can send any message from server to any client. If client is following the instruction, It is ok otherwise we can shutdown the client PC form server side

REFERENCES

[1] Camilo, Viecco. ―Improving Honeynet Data Analysis,‖ Information Assurance and Security Workshop, pp. 99-106, 2007.

[2] D. Moore, ―Network telescopes: Observing small or distant security events,‖ Proceedings of the 11th USENIX security symposium, 2002.

[3] D. Moore, C. Shannon, G. Voelker, and S. Savage, ―Network telescopes: Technical report,‖ CAIDA, April, 2004.

[4] Dacier M, Pouget F, Debar H. Honeypots: practical means to validate malicious fault assumptions. In: Proceedings of 10th pacific rim international symposium on dependable computing, pp.383–8, March 2004.

[5] Eugene Spafford. An analysis of the Internet worm. In Proceedings of European Software Engineering Conference, September 1989.

[6] Evan Cooke, Michael Bailey, Z Morley Mao, David Watson, Farnam Jahanian, and Danny McPherson. Toward understanding distributed blackhole placement. In Proceedings of the Second ACM Workshop on Rapid Malcode (WORM), October 2004.

[7] http://www.pandasecurity.com.

[8] http://www.sans.com.

[9] J. Dike, ―User-mode linux,‖ Proceedings of the 5th annual conference on Linux Showcase & Conference-Volume 5, USENIX Association Berkeley, CA, USA, pp. 2-2, 2001.

[10] Khattab M, Sangpachatanaruk C,Mosse D, MelhemR, Znati T. Roaming honeypots formitigating service-level denial-of-service attacks. In: Proceedings of the IEEE 24th international conference on distributed computing systems March, p. 328–37, 2004.

[11] Krawetz N. Anti-honeypot technology. IEEE Security & Privacy Magazine, Vol. 2(1), pp. 76–9, 2004.

