Worm Signature generation using Honeypot Technology

Avijit Mondal, Anoy Chowdhury and Dr. R.T Goswami

Abstract: In cyber world, the major problem is to detect malicious objects mainly newly invented programs. Though there is some pre-used methodology to detect old attacks, because they have previous signature generation approach. But when a new attack comes in situation, it's very difficult to detect the attack pattern.

In this paper we have proposed a methodology to detect malicious objects specially worm attacks and a proposed algorithm to generate signature for Worm. Our proposed technique is optimal cost technique too. We have used Double-Honeypot architecture to implement the technology.

Keywords: Honeypot, Malicious objects, Worm, Double-Honeypot

Introduction: We know that malicious objects are an important issue in modern days security. we can take an approach to detect this malicious activities. Let there is an e-mail server which is responsible to send and receive the e-mails of the persons in an organization. As, all of us know that e-mail is a big carrier of malicious attacks. To detect e-mails having such attacks, we can have a tricky way. We can create dummy e-mail account having no restrictions to receive e-mails. We do not forward this account to any one for the communication. As the e-mails having malicious attacks are forwarded to all the e-mail accounts at this e-mail server, so, for dummy account also. Therefore, to detect worm attacks we simply check the dummy account first because e-mails received in this account will be having maximum probability of worm attack. To save the network form such worm attacks we delete all the e-mails from all the e-mail accounts at this server [1]. Honeypot works like that. Honeypot is an information resource whose value lies in unauthorized or illicit uses of that resource [2]. Anything will come through a honeypot will be taken as an attack or probe. It is generally two types. High interaction and low interaction honeypot. High interaction honeypot gives the user access to the real operating system where nothing is restricted. Honeynet is an example of high interaction honeypot and low interaction honeypot does not provide any security, only it collects information about the attack. Honeyd is an example of low interaction honeypot.

Extended Double-Honeypot architecture: The idea of double honeypot system is inbound honeypot is not authorized to make an outbound connection [3]. As we are much concern about worm attacks because worm has its self replication property, it can replicate very easily to the intended machine, we are proposing this double honeypot system architecture. When an attack comes into inbound honeypot it tries to make an outbound connection because of its replication property and all the attack signature are transferred to the low interaction honeypot[4]. We are using worm replication property to generate signature. Figure 1 illustrates Double Honeypot Architecture.

But we also know that intranet is a connection of more than one LAN. These distinct LANs may have different vulnerable systems. Now in this situation if we design architecture of Honeypot for whole intranet it will be very difficult to implement [5]. For this we have used Extened architecture with sticky honeypot concept and Figure 2 describes this architecture.

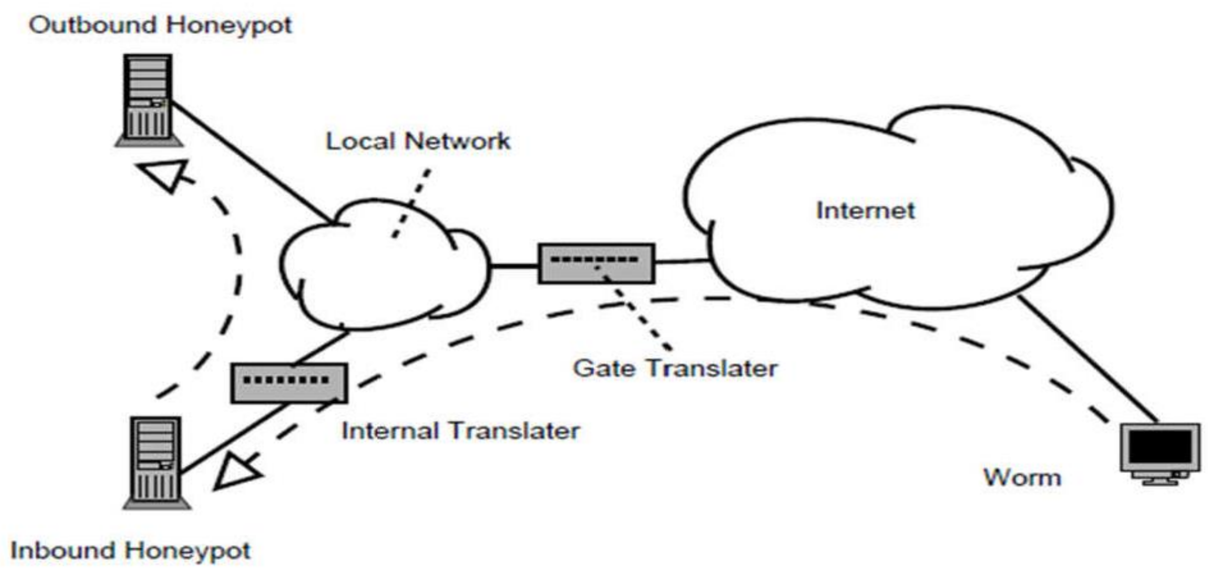

Fig. 1. Using double-honeypot detecting Internet worms

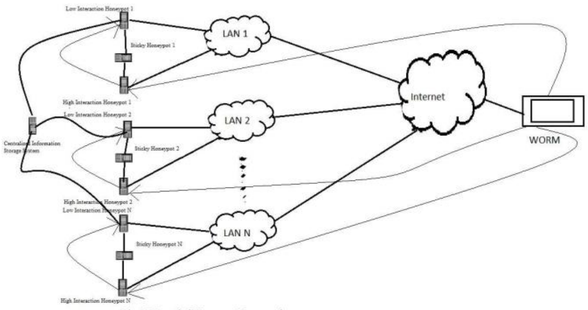
Low Interaction Honeypot 1
LAN 1
Sticky Honeypot 1
High Interaction Honeypot 1
Low Interaction Honeypot 2
LAN 2
Internet
WORM
Centralized Information Storage System
Sticky Honeypot 2
High Interaction Honeypot 2
Low Interaction Honeypot N
LAN N
Sticky Honeypot N
High Interaction Honeypot N

Fig. 2. Extended Honeypot Framework

Signature generation approach for Worm using Honeypot:

To generate automated signature we have used Antivirus Engine which consist of behavioural detection engine and 3 High Interaction Honeypot and 1 Low Interaction Honeypot. We have also used Sticky Honeypot to slow down worm propagation rate, such that signature generator can get more time to analyze the attack pattern. Figure 3 illustrates the system architecture of signature generator.

Proposed Algorithm:

1. Gate translator will collect all the traffic and will redirect them to the first Inbound Honeypot.

2. Internal translator will redirect the malicious traffic to the second Inbound Honeypot.

3. Sticky honeypot is adjusted between Honeypot 1 and Honeypot 2 to slow down the worm propagation rate. Different TCP tricks are there for Sticky Honeypot.

4. Honeypot 3 consists of Antivirus Engine. All the malicious traffic will go through the Engine and it consist of behavioural detection engine and corresponding signature will be generated and will go through a Low Interaction Honeypot.

5. Low Interaction Honeypot will send the signature to a centralized storage system through which IDS can get the information. So analyzing the signature IDS can protect any attack, as it will get its generated signature.

6. If the Antivirus Engine in Honeynet 3 unable to detect any Signature then that payload will be automatically redirected to internet through unused IP system.

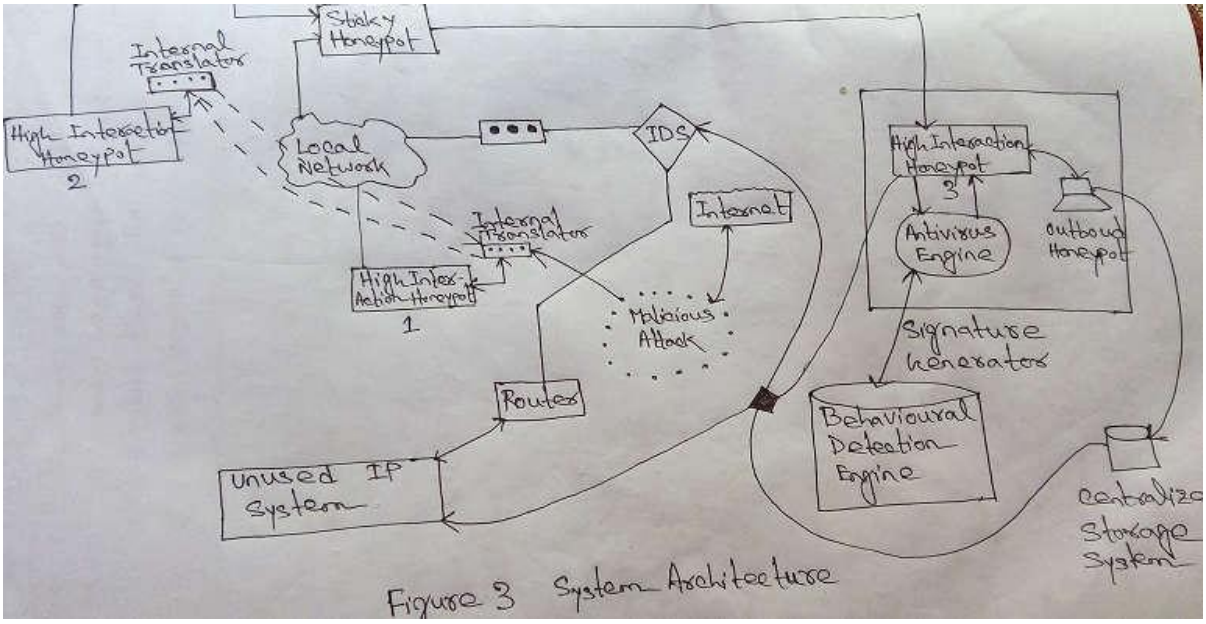

Figure 3 System Architecture

Conclusion: The paper provides an idea about honeypots and their usage. As honeypots is relatively a new technology and having good scope for future works. Honeypot can be used with well established security tools such that IDS or Firewalls to make them more effective. Malicious program can be easily detected by honeypot technology concept.

We have also used Extended-Double-Honeypot Architecture to detect malicious programs like worm attack. These technologies are new and have a very good prospect in market because it examines a malicious code which is not seen before. Substring Extraction from worm signature is also a popular methodology to detect signature pattern[6].

Reference:

[1] Zhou, J.; Heckman, M.; Reynolds, B.; Carlson, A.; Bishop, M. (2007). Modeling network intrusion detection alerts for correlation. ACM Transactions on Information and System Security (TISSEC), Volume 10, Issue 1, pp.-1-31.

[2] Yong Tang, Shigang Chen," An Automated Signature-Based Approach against Polymorphic Internet Worms," IEEE Transaction on Parallel and Distributed Systems, pp. 879-892 July 2007.

[3] Bio Intrusion Detection System. Available: http://www.bro-ids.org/, 14 February 2011. International Journal for Information Security Research (IJISR), Volume 1, Issues 1/2, March/June 2011 Copyright

[4] B.K.Mishra., N.Jha., SEIQRS model for the transmission of the malicious object in computer network, Applied Mathematical Modeling, 34, pp.710-715,2010.

[5] Yong Tang and Shigang Chen., Defending Against Internet Worms: A Signature- Based Approach, Department of Computer & Information Science & Engineering, University of Florida, Gainesville, FL,USA., pp. 32611-6120,2010.

[6] Tang,Y.; Chen, S. (2005). Defending Against Internet Worms: A Signature-Based Approach. In Proceedings of IEEE INFOCOM‟2005, Miami, Florida, USA, pp.1-1

CALL FOR PAPERS

The TIU Transaction on Intelligent Computing (TTIC) journal publishes peer-reviewed original works that advances the prospects of intelligent computing by presenting emerging discoveries, important insight and surveys (tutorial) in fields ranging from Machine Intelligence, Artificial Intelligence to Soft Computing and Neural Network. The journal comes out with new volume every year and intends to attract papers that justifies the objectives entailed within these tenets of intelligent computing.

The TTIC invites academicians, researchers, scholars, authors, and industry experts to submit their novel endeavors, enterprising solutions and innovative insights that advances the scope and prospects of intelligent computing for its upcoming volume to be published in the month of December 2019.

Subjects covered within the scope of the journal are interdisciplinary in nature and broadly includes:

Soft Computing | Artificial Intelligence | Mobile Computing | CPUT Computing | Fog Computing | Machine Learning | Image Processing | Security System | Cyber Security | Big Data Analytics | Cyber Security | Internet Service Application | Internet Communication | Computing-Vision | Control System | VLSI Design | Bioinformatics | Robotics | Mathematical Innovation | Algorithm | Atmospheric Physical Engineering

All papers submitted to the journal will undergo extensive blind-peer review process prior to acceptance.