Detection and Analysis of Network & Application Layer Attacks using Honeypot with System Security Features

Prof. Kothawale G. S[1] Sanket Tambe[2] Akshay Harale[3]
[1]Assistant Professor & Head of Dept. [2,3]BE Student
[1,2,3]Department of Computer Engineering
[1]Al-Ameen College of Engineering, Pune, 412216, India & AAEM'F COE, Koregaon Bhima, Pune 412216 India [2,3]AAEM'F COE, Koregaon Bhima, Pune 412216 India

Abstract— Information related security in the sense of end user interactions has become a one of the most top priority in digitalized modern world in coordinate to the new and latest technological developments. Many approaches, tools, and expertise are used to provide the information security to the information systems. Honeypot is an active defense system for network security. It is able to traps raid, record intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Integrated with the other security solutions, the honeypot is able to solve many traditional dilemmas. We expatiate key segments of data capture and data control in a honeypot and give a classification for honeypot according to security goals and application goals. Honeypot is Java based deception tool having influential services (FTP etc.), it is a "Rule & Anomaly" based intrusion detection engine and a network-based administration and monitoring tool. This paper analysis the attack detector with existing system drawback which presents proposed approach more efficiently. Additional system security features are also added based on accessing the system securely. Features like detection of an intruder based on the time stamp and log-in details are considered. Tracking of the user is based on the system log and other databases pre-defined for secure accessing.

Key words: Network Security, Intrusion Detection System, Honeypot

I. INTRODUCTION

A honeypot is a closely monitored and analyzed computing resource that has a sole purpose to be intruded, probed attacked, or compromised. A honeypot is defined as "An information system resource whose value lies in the unauthorized or illegal use of that resource". A honeypot can capture every action by the intruder or attacker that is made inside the honeypot. A honeypot is able to create a log of access attempts by an intruder, capture the keystrokes, identify less accessed and modified files or folders, and identify the programs that are executed within the honeypot. If an intruder is unaware that he is inside a honeypot, we can even identify his motive behind the attack. Honeypots can be comfortably placed inside of the network, outside of the network and also inside DMZ (Demilitarized Zone). They can even be placed in all of the above locations. Honeypots are essential in learning how intruders and attackers probe and attempt to gain access to your systems. By learning and recording how intruders and attackers explore and manipulate the system to gain access, we can gain the perception of attack methodologies that helps us to protect our real production systems.

Honeypots are also required to record the data and provide forensic information analysis of an attack to government law enforcement agencies. These archives created by the honeypots are required to impeach the intruders or attackers. Honeypots are the security resource whose and significance lies in being prodded, attacked, or compromised. They can be real operating systems or virtual environments imitating the real production systems. Honeypots are mostly the best computer security- protection tool for the job. They can be used as an assistant tool to log and prevent hacking attacks. Honeypots are presently in the second formal stage of development, known as GenII. GenII honeypots use inline IDSs for flexible data control. Hacking attacks can also be manual, automated, or combined. Honeypots are not just the "install and forget it "systems. There are several steps in the systems that you can use to lower the legal risks from using a honeypot

II. RELATED WORK

Honeypot is a powerful technology. It has a very high potential. It detects every new attack. This research is completely focused on identifying, researching and capturing new threats. The attack can be malicious and dangerous, the attack is random with an attacker in how many system they can break into and which system it break. Insider threat is more dangerous than the external threat. And for identifying those thread. In this paper, many ideas are discussed in regards with ARDA Liber Indication. This area examines the rudiments of Honeypot and clarifies to sum things up the prerequisites for which honeypot has been created.

A large portion of the Honeypot depend on checking Network or OS level assaults, however, the confinement with this system is assault can straightforwardly go through the system level security. The interloper can pass pernicious code to the web application level through the Firewall and IDS as these layers are utilized to limit access to an application, yet don't have any insight with respect to the data coursing through them to the web application, where they can misuse the vulnerabilities in the application. The paper proposes to broaden the convenience of honeypots to web applications.

III. PROPOSED SYSTEM

The main stage is to achieve a casualty, which intends to send a correspondence endeavor to a particular administration facilitated on a system gadget. For instance, a strategy for an aggressor to find countless is to examine incrementally all system addresses inside a particular subnet. The aggressor goes to the following stage just if the casualty answers and the administration are interested in the assailant.

The second stage is to abuse the administration found on the casualties machine by propelling an assault payload. There is not generally a reasonable limit between the first and second stage, on the grounds that a few assaults are

made of a solitary system parcel, so correspondence endeavors what's more, assault payload cover. Besides, assailants regularly utilize the association instated amid the output to send the assault payload. The assailant goes to the following stage as it were in the event that the administration is effectively traded off by the assault propelled.

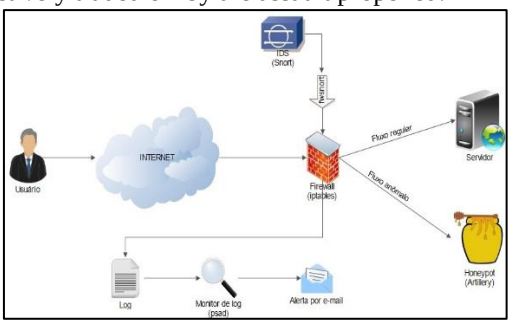

Fig. 1: Proposed System

The third stage is to utilize the recently defiled casualties machine. The assailant can be somebody who needs to access a particular asset, or a worm that is just spreading from one powerless machine to another. In such case, the worm introduced on the recently defiled machine will begin examining for different casualties and will make another assault procedure beginning with stage one once more. From this model, we can outline distinctive periods of system assault with the diverse sorts of honeypots. Figure subtle elements this mapping and clarifies how honeypots properties are connected.

In the event that a system association is accurately settled between the two companions. As we just observed while clarifying the second period of an assault, we can discover a few special cases to this prerequisite, since a few assaults are made of a solitary system bundle that does not require initial affirmation from the casualty to be sent. Low collaboration honeypots are appropriate to accumulate abuses sent amid the second period of an assault since they are adaptable and give enough cooperation to the assailant to send its assault payload. Be that as it may, copied scripts facilitated by low cooperation honeypots won't generally fulfill the level of collaboration required by complex assaults. This limit amongst straightforward and complex assaults is spoken to by the level of imitating. Besides, low collaboration honeypots can't be bargained by aggressors, so the third period of the assault procedure is never gathered by this write off design.

IV. PSEUDO CODE

AES is another cryptographic calculation which can be utilized to secure electronic information. AES is a piece figure of symmetric-key which are utilize the keys of 128, 192, and 256 bits, and scrambles and in addition decodes substance in pieces of 128 bits. AES utilize a keys pair, the same key use by the symmetric-key figures to encryption and decoding of information. The same number of bits have the information which encoded which got by square figures that the information had. A circle structure use by Iterative figures that changes and substitutions of the information perform over and again.

A. Algorithm

1) For each round, AES needs an alternate 128-bit square of round key additionally one more.
2) Add Round Key with a square of the round key, every byte of the state is consolidated utilizing bitwise xor.
3) Rounds
– Sub Bytes in this progression every byte is supplanted with another byte.
– Shift Rows for a specific number of steps, the states last three columns are moved consistently.
– Blend Columns on the segments of the state a blending operation works, in each segment joining the four bytes.
4) Add Round Key
5) Final Round (no Mix Columns)
– Sub Bytes
– Shift Rows
– Add Round Key.

V. SIMULATION RESULTS

Figure below shows,

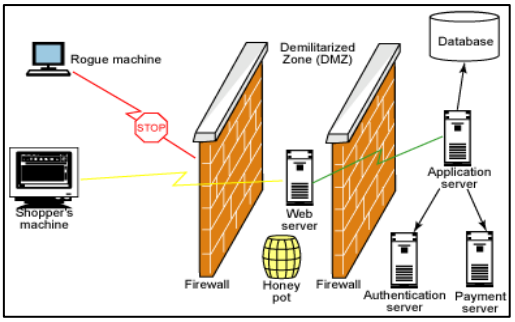

Fig. 2: Simulation results

Here we perceive how they can be utilized as a major aspect of system security technique and the improvement of honeypot named Maya. This honeypot gives movability, a powerful logging component, an electronic instrument for administrating cum checking of Honeypot and another arrangement of standards for investigation of utilization level assaults.

VI. EVALUATION TABLE

Attributes	Existing system	Proposed system
Security	Less secure	Most secure
Access	Fine-grained access is not provided	Fine grained access is provided
Speed	Low	High
Flexibility	Not flexible	Flexible

Table 1: Simulation Results

VII. OUTCOME

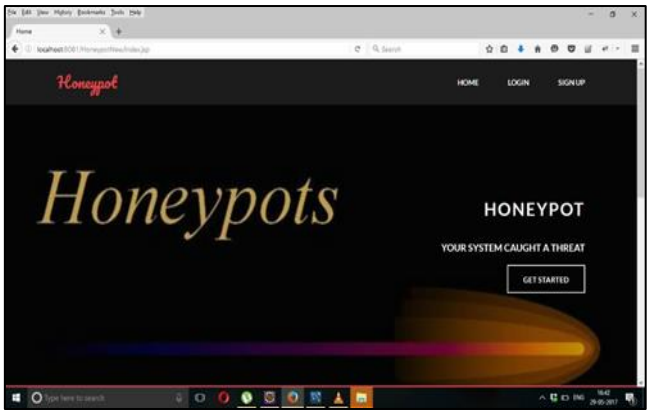

Fig. 3: Home Page

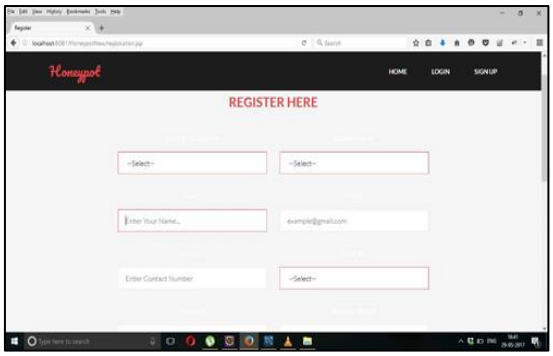

Fig. 4: Register page

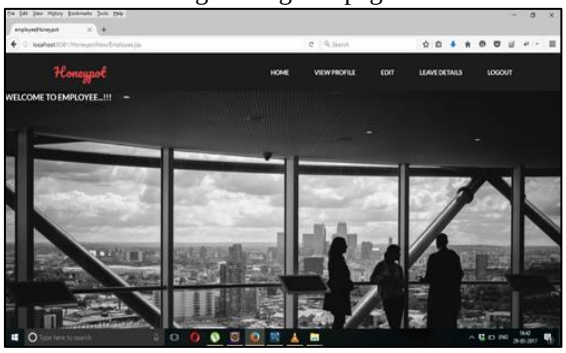

Fig. 5: Login page

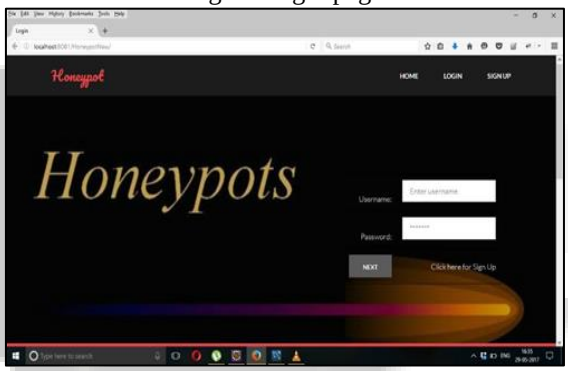

Fig. 6: Employee's Home Page

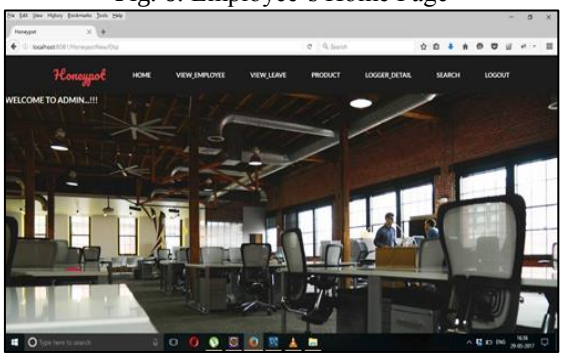

Fig. 7: Admin Page

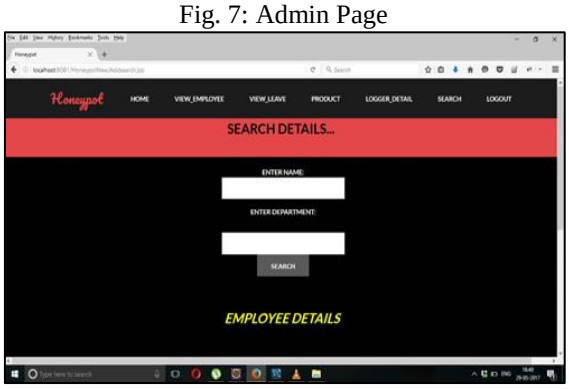

Fig. 8: Search page

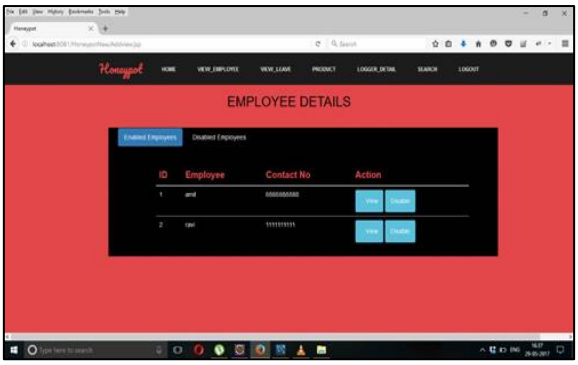

Fig. 9: Employee detail Page

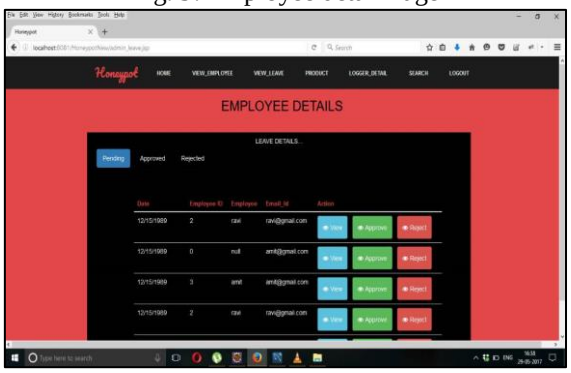

Fig. 10: Leave approval page

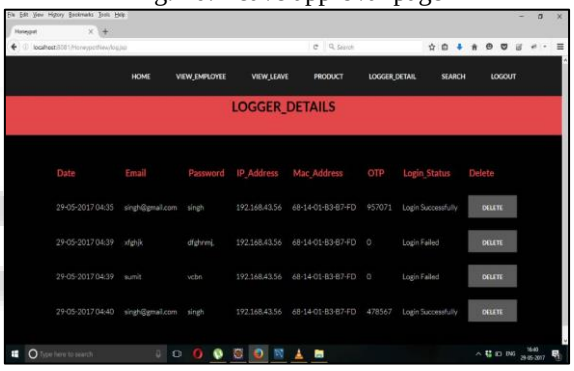

Fig. 11: Logger detail page

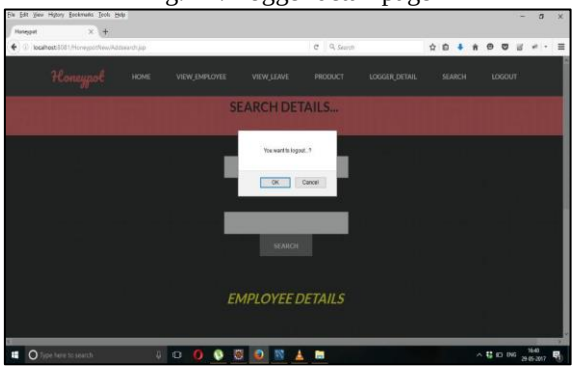

Fig. 12: Log Out page

VIII. CONCLUSION AND FUTURE WORK

Here we perceive how honeypot can be utilized as a major aspect of system security technique and the advancement of honeypot named Maya. The honeypot gives versatility, a vigorous logging component, an electronic device for administrating cum observing of Honeypot, what's more, another arrangement of tenets for investigation of use level assaults (SQL-Injection Cross program scripting and so on).

REFERENCES

[1] Cohen, Fred. "A note on the role of deception in information protection." Computers and Security 17, no. 6: 483-506. 1998.
[2] F-Secure. F-secure Corporations data security summary for 2003 the year of the worm. Technical report 2003.
[3] Spitzner, Lance. "Honeypots: Catching the insider threat." In Computer Security Applications Conference, Proceedings. 19th Annual, pp. 170-179. IEEE, 2003.
[4] Provos, Niels. "A Virtual Honeypot Framework." In USENIX Security Symposium,vol. 173. 2004.
[5] A Game Theoretic Model for Enabling Honeypots in IoT Net- works, Tony Q.S. Quek and Jemin Lee, 2007
[6] La Spitzner, Lance. "The Value of Honeypots, Part One: Definitions and Values of Honeypots, 2010"A note on the role of deception in information protection." Computers and Security 17, 2010
[7] Ant-based distributed denial of service detection technique using roaming virtual honeypots, Rajalakshmi Selvaraj,2010
[8] Detecting and Analyzing Zero-Day Attacks Using Honeypots Constantin Musca; Emma Mirica; Razvan Deaconescu, 2013 Detection and Analysis using Honeypot
[9] A software router based predictive honeypot roaming scheme for network security and attack analysis Asit More, 2013
[10] An automated bot detection system through honeypots for large-scale Fatih Halta; Erkam Uzun; Necati ieci; Abdulkadir Poul; Bakr Emre Cyber Conflict, 2014
[11] Honeypots deployment for the analysis and visualization of malware activity and malicious connections Ioannis Koniaris; Georgios Papadimitriou; Petros Nicopolitidis, IEEE International Conference on Communications, 2014
[12] Distinguishing betweenWeb Attacks and Vulnerability Scans Based on Behavioral Characteristics Katerina Goseva-Popstojanova, 2014
[13] Multi-stage Attack Detection and Signature Generation with ICS Honeypots S.Emmanouil Vasilomanolakis, 2014
[14] Malicious traffic detection in a private organizational network using honeynet system Rupinder Kaur; Er. Sunil Nagpal; Saurabh Chamotra, 2015
[15] Detection and Analysis of Network and Application layer Attacks using Maya Honeypot, Seema Sharma,2015
[16] Deceptive Attack and Defense Game in Honeypot-enabled Net- works for the Internet of Things ,Quang Duy La, Member , 2015

