Virtual CMS Honey pot capturing threats In web applications

[1] BADI ALEKHYA, ASSITANT PROFESSOR, DEPT OF CSE , T.J.S ENGINEERING COLLEGE

Abstract--Now-a-days various types of attacks on different websites have increased drastically . This has led to raising interest for more aggressive forms of defence to improve the security and existing methods. One of these methods involves the use of honeypots. Generally it consists of a computer, data, or a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. A honey pot is a security resource whose value lies in being probed, attacked or compromised. In this paper, we provide an overview of honeypots and explain about some traditional tools which can be used for website security, and early threat detection. Open source Content Management System(CMS) is used by web administrators. Web applications have increasingly been the focus of attackers of the unintentional web vulnerabilities that comes from the new introduced functionality .

Index Terms: CMS (Content Management System), Honey pot, High-interaction ,Honey pot, security, Threats, Virtual Honeypot,Vulnerabilities

A.INTRODUCT ION:

Web applications have become an integral part of our daily life . Most of the services are accessed through internet only, and insecurity here may result in compromised data due to attack by attackers or intruders. They can easily enter into the system and hack personal data by developing different tools like viruses, worms, Trozan horse etc, and hence traditional tools of network security face many problems to identify these different kinds of attacks . help us in tracking One of the important tools used for threat detection is Intrusion Detection System (IDS). It is a device or/and software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management System. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.But, Intrusion Detection System (IDS) can't identify the new kind of attacks. Information of unknown signature of intrusion in IDS can't be detected until the attacks are analyzed. To detect, to prevent the intrusion in the existing system, as firewall also cannot identify the new intruder who has connected to the network. With a proxy server, users can login

to firewall and then access the network. But other security tools such as firewall and IDS are completely passive for that their task is to prevent or detect attacks. Hence we need a system that can the threats actively.

B.DEFINITION OF HONEYPOT

"A honeypot is a resource whose value lies in being probed, attacked or compromised." Honeypots is a technology whose value lies in the "bad guys" interacting with it. Honeynet is a network that contains one or more honeypots which is connected. It is a high interaction honeypot that is designed to capture extensive information on threats. It deployed in real systems, applications and services.

Honeypots are closely monitored network decoys serving several purposes:

- Early threat detection.
- Actively detects future threat &possible vulnerabilities in existing system.
- Adversary identification.

Virtual honeypot is defined as the honeypot which is to be installed and maintained in an particular system/server.

C.CLASSIFICAT ION OF HONEYPOT

Honeypots can be classified based on their purpose (production, research) and level of interaction (low, medium, high) [6].

C.1 PURPOSE OF HONEYPOT S

C.1.1 PRODUCTION HONEYPOT

A production honeypot is one used within an organization's environment to protect the organization

*C.*1.2RESEARCH HONEYPOT

A Research honeypot is primarily for learning new attacking methods and tools, gaining new information about attacks though it can be used for production honeypot [1]. It also gains information about the black hat community and does not add any direct value to an organization. They are used for collecting general threats in organization. Its main function is to study the way in which the attackers enter and establish their way of attack, it helps to understand their motive and behavior. Research honeypots are complex, both to deploy and to maintain and capture extensive amounts of data. These are typically used in large organizations such as governments, universities, large corporations interested in learning more about different types of threats

.Research honeypots also add to research by providing study case security, cyber threats. They help to record how the attacker compromised the system in a step by step manner.

In honeypot once an attack has been detected the machine can be pulled offline and attack can properly studied in order to provide counter measures for security.

C.2LEVEL OF INTERACTION OF HONEYPOT

The level of interaction is defined as the range of attack possibilities that a honeypot allow an attacker to system. These levels are Low-interaction honeypot, Medium interaction honeypot, High-interaction honeypot [4].

C.2.1LOW-INTERACTION HONEYPOT

On lo w-interaction honeypot, there is no operating system that an attacker can operate on [7]. They can be compromised to passive IDS since they do not modify network traffic in any way and also it cannot interact with the attacker.

Low-interaction honeypots are the easiest to install, configure, deploy, and maintain because of their simple design and basic functionality [1]. Typical use of low-interaction honeypot includes: port scans identification, generation of attack signatures, trend analysis and malware collection. For example, a low-interaction honeypot could emu late a standard UNIX server with several running services, such as Telnet and FTP.An attacker could Telnet to the honeypot, get a banner that states the operating system, and perhaps obtain a login prompt. The attacker can then attempt to login by brute force or by guessing the passwords. The honeypot capture and collect these attempts, but there is no real operating system for the attacker to log on to. The attacker's interaction is limited to login attempts. It has the lowest level of risk Lo w-interaction honeypots can identify the following functions:

Time and date of attack.

Source IP address and source port of the attack.

Destination IP address and destination port of the attack.

Example of low-interaction: Honey

C.2.2MEDIUM-INTERACTION HONEYPOT

Medium-Interaction honeypots are slightly more sophisticated than low-interaction honeypots, but less sophisticated than high-interaction honeypots [12]. These are usually more time consuming to install and configure than low-interaction honeypots. Deploying and maintaining medium-interaction honeypots is complicated process than working with lo w interaction solutions [1]. Attackers have greater interaction, so we must deploy this interaction in a secure manner. Medium-interaction honeypots also have greater complexity, and that increase the risk that something could go wrong. Unlike simple port scans, we can capture worm payloads or attacker activity, learn what happens after attackers gain access to a system and how they elevate privileges, and even capture there toolkits. This greater level of interaction comes with more work and greater risk, but it reward us with a large amount of information. Some examples of medium interaction Honey pot include mw collect, nepenthes and honey trap. Mw collect and nepenthes can be used to collect autonomously spreading malware. Honey trap dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks.

C.2.3HIGH-INTERACT ION HONEYPOT

High-Interaction honeypots are the extreme of honeypot technologies. They give us vast amount of

information about attackers, but they are extremely time consuming to build and maintain. High-interaction honey pot gives the attacker access to a real operating system where nothing is emulated or restricted. This kind of honey pot must have a robust containment mechanism in order to prevent, once compromised, its use to attack other networks. A variety of different technologies are involved, such as firewall or IDS. All of the technologies have to be properly customized for the high-interaction honeypot. Complexity becomes high level of risk.

Example of High-interaction honey pot: Honey net.

D. HONEYNET

Honey nets are high-interaction honey pots. Attackers can probe, attack, and exploit any system within the honey net, giving them full operating systems and applications to interact with [3]. The systems within a honey net can be anything: a Solaris server running an Oracle database, a Windows XP server running on IIS web server, a Cisco router [1].In short, the systems within a Honeynet are true production systems.

E. HOW HONEYNET S WORK

Honey net is a simple mechanism that utilizes principle of honey pots in a network. Anything sent to Honey net is suspect, potentially a probe, scan, or even an attack [5]. Anything sent from Honey net implies that it has been compromised an attacker or tool is launching activity. Honey nets take the concept of honey pots one step further; Instead of a single system, a Honey net is a physical network of multiple systems [1].There are three critical elements to Honey net architecture; data control, data capture, and data collection.

Data Control concerns protecting other networks from being attacked and compromised by computers on the Honeynet. The process of Data Control must be automated to prevent the hacker from getting suspicious. Data Capture concerns information. All information that enters or leaves the honey net must be collected for analysis. It is to prevent the hacker from bypassing the honey net network. The data that is collected must be stored in a location different from the Honey net. Data Collection is unique in that it is not a requirement for stand alone. Honey net deployments. The purpose of data collection is to centrally capture and aggregate all the information multiple Honeynets collect.

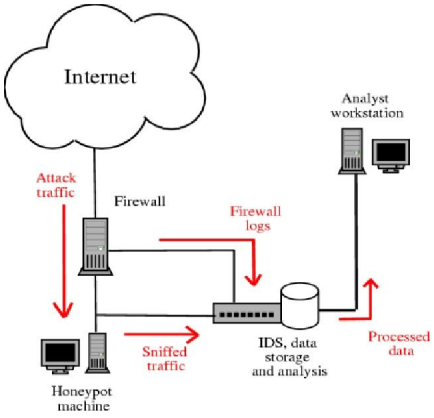
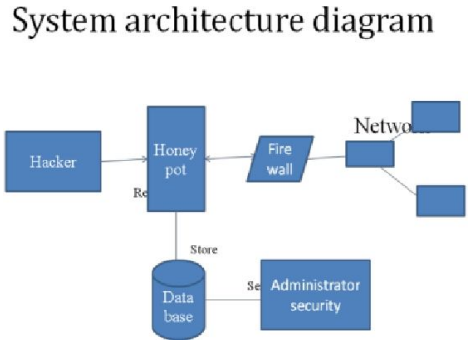


Fig. 1 Sample Honeynet Setup

Fig 1 shows the architecture of Honey net. In this architecture [10] request is sent from the intruder. Then the firewall logs as the attaches the system enters and store in the data storage and analysis section for further purpose. The collected data is analyzed by the analyzer. In IDS and analysis machine having some of the Snort NIDS which is for the data analyze about threats.

F.SYST EM ARCHITECTURE



The architecture explains about the total function which will happen. First of all the user or hacker sends an request to the server or web request. Then the request is send to the particular server. Then the request is sent to the systems which are connected to that server.

Then the honey pot respond to that request it will give results like the original interaction be going with the server it makes to feel the user. Then that detail is entered into the database which maintains the log list of the requests. Then this data base be verified and

provide more security by administrator.

The log details are sent to firewall for future purpose of identification of new threats for to block. Fro m firewall the request be sent to network who is authorized address only it will allows. Administrator

will test the requests and maintain the network by providing more security.

G. CONCLUSION

In this paper we provide a brief explanation of what honey pots are, and what they useful. Explained about the virtual honey pot. Virtual Honeypot are new technology which is to be using for to give the network security from threats for organizations .

REFERENCES

1. Honeypots: Tracking Hackers by Lance Spitzner, published Sep13, 2002
2. Spitzner, Open Source honeypots: Learning with Honeypot
3. Spitzner, The value of Honeynets at chapter11, 2002.
4. Honeypots: Concepts, Approaches, and Challenges by Iyatiti Mokube, Michele Adams.
5. The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks, proceedings of the 2003 IEEE, workshop on Information Assurance.
6. http://www.spitzner.net
7. Baumann, R. and Platner, C. White Paper: Honeypots, Swiss Federal Institute of Tech, 2002.
8. http://www.honeypots.net/.

   Honeypot: A supplemented active Defense System for Network Security.
9. http://old.honeynet .org/scans
10. http://www.chuvakin.org