HONEYPOTS OF SECURITY SYSTEM TO IDENTIFY BLACKHAT COMMUNITY IN NETWORK

Juili J.Kotangle[1],Supriya V.HumaneRoshani[2],A. BomratwarSneha[3], P. Narule[4], Aditi R. Pawar[5]
Department of Computer technology
K.D.K.C.E, Nagpur

***Abstract:-*Honeypot is used in the area of computer and Internet security. It is a resource, which is intended to be attacked and computerized to gain more information about the attacker, and used tools. One goal of this paper is to show the possibilities of honeypots and their use in research as well as productive environment. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts. Honeypots provide a platform for studying the methodsand tools used by the intruders (blackhat community),thus deriving their value from the unauthorized use oftheir resources. This paper would first give a brief introduction to honeypots-the types and its uses. We will then look at the other components of honeypots and the way to put them together. Finally we shall conclude by looking at what the future holds for honeypots.' Honeypot is used in the area of computer and Internet security. It is a resource, which is intended to be attacked and computerized to gain more information about the attacker, and used tools. One goal of this paper is to show the possibilities of honeypots and their use in research as well as productive environment. Compared to an intrusion detection system, honeypots have the big advantage that they do not generate false alerts. Honeypots provide a platform for studying the methodsand tools used by the intruders (blackhat community),thus deriving their value from the unauthorized use of their resources. This paper would first give a brief introduction to honeypots-the types and its uses. We will then look at the other components of honeypots and the way to put them together. Finally we shall conclude by looking at what the future holds for honeypots.'**
In the past several years there has been extensive research into honeypot technologies, primarily for detection and information gathering against external threats. However, little research has been done for one of the most dangerous threats, the advance insider, the trusted individual who knows your internal organization. These individuals are not after your systems, they are after your information. This presentation discusses how honeypot technologies can be used to detect, identify, and gather information on these specific threats.

Index Terms: Blackhat, Honeypot, Security, Network, etc

I. INTRODUCTION:-Global communication is getting more significant every day. At the same time, computer crimes are growing rapidly. Counter measures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. As in the military, it is important to know, who your enemy is, what kind of strategy and plan he uses, what tools he utilizes and what he is aiming for. Gathering this kind of information is arduous but important. By knowing attack strategies, countermeasures can be improved and anomalies can be fixed. To gather as much information as possible is one main target of honeypot.

Generally, such information gathering should be done without the attacker's knowledge. All the gathered information provides an advantage to the defending side and can therefore be used on productive systems to prevent attacks. Honey pots are an exciting new technology. A honeypot is a resource whose value is in being attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited.

resources. Security is broke down into three categories as follows [1].

Prevention: We want to stop the bad guys. If you were to secure your house, prevention would be similar to placing dead bolt locks on your doors, locking your window, and perhaps installing a chain link fence around your yard. You are doing everything possible to keep the threat out.

Detection: We want to detect the bad guys when they get through. Sooner or later, prevention will fail. You want to be sure you detect when such failures happen. Once again using the house analogy, this would be similar to putting a burglar alarm and motion sensors in the house. These alarms go off when someone breaks in. If prevention fails, you want to be alerted to that as soon as possible.

Reaction: We want to react to the bad guys once we detect them. Detecting the failure has little value if you do not have the ability to respond. What good does it to be alerted to a burglar if nothing is done? If someone breaks into your house and triggers

the burglar alarm, one hopes that the local police force can quickly respond. The same holds true for information security. Once you have detected a failure, you must execute an effective response to the incident.

Value of Honeypots in each of the categories:-Honeypots have certain advantages and disadvantages as security tools. It is the advantages that help define the value of a honeypot. The beauty of a honeypot's lies in its simplicity. It is a device intended to be compromised, not to provide production services. This means there is little or no production traffic going to or from the device. Any time a connection is sent to the honeypot, this is most likely a probe, scan, or even attack. Any time a connection is initiated from the honeypot, this most likely means the honeypot was compromised. As there is little production traffic going to or from the honeypot, all honeypot traffic is suspect by nature. Now, this is not always the case. Mistakes do happen, such as an incorrect DNS entry or someone from accounting inputting the wrong IP address. But in general, most honeypot traffic represents unauthorized activity. As we discussed earlier, there are two types of honeypots, production and research. We will first discuss what a production honeypot is and its value. Then we will discuss research honeypots and their value. **General Model for Honeypot:-** We interpret two essential requirements **of** honeypot data control and data capture. The following model fulfils the basic two requirements and performs effectively. We deploy IDS component, firework component, router control component, log component. In the general model, target OS and applications with default configured. All of them cooperate one another to form a honeypot system. We will analyze it how to work and fulfil two requirements [2].

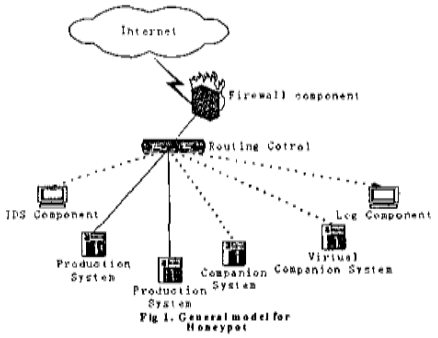


Fig 1. General model for Honeypot

II. RELATED WORK:-Characterizing attacker's activities present in honeypot traffic data can be challenging due to the high dimensionality of the data and the amount of traffic collected. The high amount of background noise, such as scans and backscatter, add to the challenge by hiding interesting abnormal activities that require immediate attention from security personnel. Detecting these outlying activities can potentially be of high value and give early signs of the discovery of new vulnerabilities or breakouts of new automated malicious codes, such as worms. In this work, we propose the use of principal component analysis (PCA), in the characterization of attacker activities present in low-interaction honeypot traffic data. PCA has been used to characterize network traffic in the past; as far as we are aware this is the first time it has been used to characterize honeypot traffic. The use of PCA in this study is motivated by the popularity of PCA as an exploratory technique that is easy to implement and requires less computational power than other linear methods, such as projection pursuit, and produces results that are easy to interpret. The effectiveness of PCA in detecting the structures of attackers activities in honeypot traffic is demonstrated through the characterization of the attackers activities into dominant groups, visualization of some the interrelationships between the extracted groups, and the ability to detect different types of outliers. Consequently, characterizing honeypot traffic will improve our understanding of attacker behaviours, optimization of honeypot design, and the identification of interesting activities. *Mirage* extends Snort a Network Intrusion Detection System ***(NIDS)*** [3]**.** Snort detects the intruder and *Mirage* redirects him to the honeypot. At the same time, it also adds intruder to the hostile IP address list and next time even if the same intruder (IP address) goes undetected by Snort, Mirage redirects him to the honeypot. The honeypot attracts and diverts the attacker from their real targets by emulating the real services. The honeypot has been made intelligent enough to emulate not only real hosts but also unused IP addresses in the LAN and provide services on them.

EXPERIENCES WITH A LOW-INTERACTION HONEYPOT: Deployment of Low interaction Honeypot The central idea of honeypots is, that any traffic directed to the honeypot, is considered an attack. In order to get an impression of what attack traffic to a honeypot actually looks like, in our work some honeypots have been set up and the results have been analyzed. To evaluate what existing honeypots are capable of, several projects of freely available honeypot software has been tested under lab conditions and in real use. The results show which approaches fit the requirements and which features are missing. Low interaction honeypots are mainly used to detect the hackers and deceive them by emulating the operating system services and port services on the host operating system. The interaction with the other hosts is limited in this type of

honeypots, which reduces the propagation of attacks. We have tested with three different honeypots under various operating systems. The first low interaction honeypot Honeyd is an open source low interaction virtual honeypot created and maintained by Neils Provos. It is intended initially for UNIX and now extended for Windows also. The second low interaction honeypot was KFSensor, a Windows based honeypot. It was deployed in a physical machine running Windows XP platform. This honeypot can emulate the ports like FTP, TCP, UDP and HTTP. The third honeypot Specter cannot monitor the unused IP address; it can only monitor the IP address assigned to the host machine.

III. EXISTING SYSTEM:-Traditional strategy is to defend ones organization as best as possible is by detecting any failures in the defence, and then react to those failures. The problem with the existing approach is that it is purely defensive; the enemy is on the attack [3]. The Data Collection also accounts in providing security. In the traditional method large amounts of data are collected which will have very low value and may or may not have significance in finding the attackers. The noise will be high in such data. It will become difficult to archive data. One of the greatest problems in security is wading through gigabytes of data to find the data you need. Many security tools can be overwhelmed by bandwidth or activity. Network Intrusion Detection Devices may not be able to keep up with network activity, dropping packets, and potentially attacks. Centralized log servers may not be able to collect all the system events, potentially dropping some events. Existing security technologies and defence system for network security are blunt while facing new attacks and intrusion. Round the clock is one of the most important properties of web application, hut attacks and intrusions changing the situation? IDS can't give alert when intrusion occurred using new signature. Even worse, we can't down the service system to check it completely because there still many online uses making their deals. To prevent, detect and react to intrusions without disturbing existing system is a severe problem for web application and network security [6]. IDS work well on detecting and alerting attacks of known signatures. Most IDS can't detect unknown intrusions. Though some can do anomaly detection by training a clean data set of normal action, clean data set is difficult or costly to get Information on Unknown signature of intrusion can't be attained unlessattacks are analyzed. It is a contradiction that laggard attaining of unknown signature and signature matching based IDS [7].

IV. ALGORITHM:-

RME (Registry management entry)

In this algorithm we edit the value of windows registry.

Technique Used:

a) ADO.net

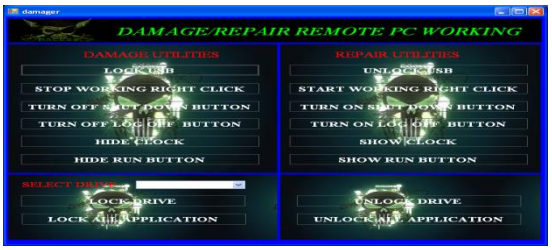
b) Registry Programming

c) Data programming

V. Snapshot:-

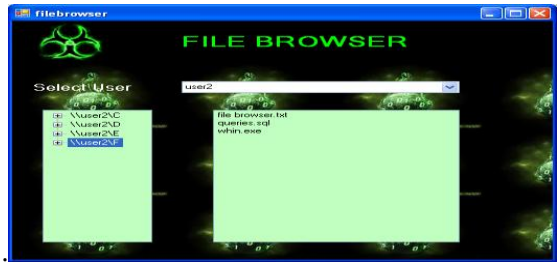
1.

2.



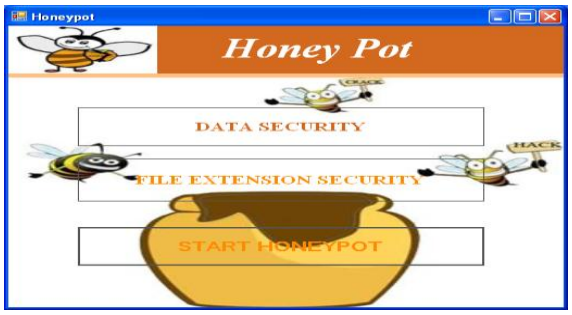
3.

4.



5.

6.



V. PROPOSED SYSTEM: -The main goals are the distraction of an attacker and the gain of information about an attack and the attacker they do attract intruders and can therefore attract some interest from the blackhat community on the network, where the honeypot is located. There are two categories of honeypots - *production honeypots* and *research honeypots.* The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization. Think of them as 'law enforcement', their job is to detect and deal with bad guys. Traditionally, commercial organizations use production honeypots to help protect their networks. The second category, research, is honeypots designed to gain information on the blackhat community. These honeypots do not add direct value to a specific organization. Instead they are used to research the threats organizations face, and how to better protect against those threats. Think of them as 'counter-intelligence', their job is to gain information on the bad guys. This information is then used to protect against those threats. Traditionally, commercial organizations do NOT use research honeypots. Instead, organizations such as Universities, government, military, or security research organizations use them.

Production Honeypot: A Production honeypot is one used within an organizations environment to help mitigate risk. It adds value to the security of production resources. Production honeypots apply to the three areas of security, Prevention, Detection, and Reaction as follows: Prevention I personally feel honeypots add little value to prevention; honeypots will not help keep the bad guys out. What will keep the bad guys out is best practices, such as disabling unneeded or insecure services, patching what you do need, and using strong authentication mechanisms. It is the best practices and procedures such as these that will keep the bad guys out. A honeypot, a system to be compromised, will not help keep the bad guys out. In fact, if incorrectly implemented, a honeypot may make it easier for an attacker to get in. Some individuals have discussed the value of deception as a method to deter attackers. The concept is to have attackers spend time and resource attacking honeypots, as opposed to attacking production systems. The attacker is *deceived into* attacking the honeypot, protecting production resources from attack. While this may prevent attacks on production systems, I feel most organizations are much better off spending their limited time and resources on securing their systems, as opposed to deception. Deception may contribute to prevention, but you will most likely get greater prevention putting the same time and effort into security best practices. Also, deception fails against two of the most common attacks today; automated toolkits and worms. Today, more and more attacks are automated. These automated tools will probe, attack, and exploit anything they can find vulnerable. Yes, these tools will attack a honeypot, but they will also just as quickly attack every other system in your organization. If you have a coffee pot with an IP stack, it will be attacked. Deception will not prevent these attacks, as there is no consciously acting individual to deceive. As such, I feel that honeypots add little value to prevention. Organizations are better off focusing their resources on security best practices.

Detection: -While honeypots add little value to prevention, I feel they add extensive value to detection. For many organizations, it is extremely difficult to detect attacks. Often organizations are so overwhelmed with production activity, such as gigabytes of system logging, that it can be extremely difficult to detect when a system is attacked, or even when successfully compromised. Intrusion Detection Systems (IDS) are one solution designed for detecting attacks. However, IDS administrators can be overwhelmed with false positives. False positives are alerts that were generated when The sensor recognized the configured signature of an "attack", but in reality was just valid traffic. The problem here is that system administrators may receive so many alerts on a daily basis that they cannot respond to all of them. Also, they often become conditioned to ignore these false positive alerts as they come in day after day, similar to the story of "the boy who cried wolf". The very IDS sensors that they were depending on to alert them to attacks can become ineffective unless these false positives are reduced. This does not mean that honeypots will never have false positives, only that they will be dramatically fewer than with most IDS implementations.

Another risk is false negatives, when IDS systems fail to detect a valid attack. Many IDS systems, whether they are signature based, protocol verification, etc, can potentially miss new or unknown attacks. It is likely that a new attack will go undetected by currently IDS methodologies. Also, new IDS evasion methods are constantly being developed and distributed. It is possible to launch a known attack that may not be detected, such as with K2s ADM Mutate. Honeypots address false negatives as they are not easily evaded or defeated by new exploits. In fact, one of their primary benefits is that they can most likely detect when a compromise occurs via a new or unknown attack by virtue of system activity, not signatures. Administrators also do not have to worry about updating a signature database or patching anomaly detection engines. Honeypots happily capture any attacks thrown their way. As discussed earlier though, this only works if the honeypot itself is attacked. Honeypots can simplify the detection process. Since honeypots have no production activity, all connections to and from the honeypot are suspect by nature. By definition, anytime a connection is made to your honeypot, this is most likely an unauthorized probe, scan, or attack. Anytime the honeypot initiates a connection, this most likely means the system was successfully compromised. This helps reduce both false positives and false negatives greatly simplifying the detection process. By no means should honeypots replace your IDS systems or be your sole method of detection. However, they can be a powerful tool to complement your detection capabilities.

Reaction:-Though not commonly considered, honeypots also add value to reaction. Often when a system within an organization is compromised, so much production activity has occurred after the fact that the data has become polluted. Incident response team cannot determine what happened when users and system activity have polluted the collected data. For example, I have often come onto sites to assist in incident response, only to discover that hundreds of users had continued to use the compromised system. Evidence is far more difficult to gather in such an environment. The second challenge many organizations face after an incident is that compromised systems frequently cannot be taken off-line. The production services they offer cannot be eliminated. As such, incident response teams cannot conduct a proper or full forensic analysis. Honeypots can add value by reducing or eliminating both problems. They offer a system with reduced data pollution, and an expendable system that can be taken off-line. For example, let's say an organization had three web servers, all of which were compromised by an attacker. However, management has only allowed us to go in and clean up specific holes. As such, we can never learn in detail what failed, what damage was done, is there attacker still had internal access, and if we were truly successful in cleanup. However, if one of those three systems was a honeypot, we would now have a system we could take off-line and conduct a full forensic analysis. Based on that analysis, we could learn not only how the bad guy got in, but what he did once he was in there. These lessons could then be applied to the remaining web servers, allowing us to better identify and recover from the attack.

Research Honeypot:- As discussed at the beginning, there are two categories for honeypots; production and research. We have already discussed how production honeypots can add value to an organization. We will now discuss how research honeypots add value. One of the greatest challenges the security community faces is lack of information on the enemy. Questions like who is the threat, why do they attack, how do they attack, what are their tools, and possibly when will they attack? It is questions like these the security community often cannot answer. For centuries military organizations have focused on information gathering to understand and protect against an enemy. To defend against a threat, you have to first know about it. However, in the information security world we have little such information. Honeypots can add value in research by giving us a platform to study the threat. What better

way to learn about the bad guys then to watch them in action, to record step-by-step as they attack and compromise a system. Of even more value is watching what they do after they compromise a system, such as communicating with other black hats or uploading a new tool kit. It is this potential of research that is one of the most unique characteristics of honeypots. Also, research honeypots are excellent tools for capturing automated attacks, such as auto-rooters or Worms. Since these attacks target entire network blocks, research honeypots can quickly capture these attacks for analysis. In general, research honeypots do not reduce the risk of an organization. The lessons learned from a research honeypot can be applied, such as how to improve prevention, detection or reaction. However, research honeypots contribute little to the direct security of an organization. If an organization is looking to improve the security of their production environment, they may want to consider production honeypots, as they are easy to implement and maintain. If organizations, such as universities, governments, or extremely large corporations are interested in learning more about threats, then this is where research honeypots would apply.

Honeypot Solutions:- The more a honeypot can do and the more an attacker can do to a honeypot, the more information can be derived from it. However, by the same token, the more an attacker can do to the honeypot, the more potential damage an attacker can do. For example, a low interaction honeypot would be one that is easy to install and simply emulates a few services. Attackers can merely scan, and potentially connect to several ports. Here the information is limited (mainly who connected to what ports when) however there is little that the attacker can exploit. On the other extreme would be high interaction honeypots. These would be actual systems. We can learn far much more, as there is an actual operating system for the attacker to compromise and interact with, however there is also a far greater level of risk, as the attacker has an actual operating system to work with. Neither solution is a better honeypot. It all depends on what you are attempting to achieve. Remember, honeypots are not a solution. Instead, they are a tool. Their value depends on what your goal is, from early warning and detection to research. Based on 'level of interaction', let's compare some possible honeypot solutions. For this paper, we will discuss six honeypots. There are a variety of other possible honeypots; however this selection covers a range of options. We will cover Back Officer Friendly, Specter, Honeyed, homemade honeypots, Mantrap, and Honeynets. This paper is not meant to be a comprehensive review of these products. I only highlight some of their features. Instead, I hope to cover the different types of honeypots, how they work, and demonstrate the value they add and the risks involved. If you wish to learn more about the capabilities of these solutions, I highly recommend you try them out on your own in a controlled, lab environment.

VI.**CONCLUSION:-**Security is a very difficult topic. The key for building a secure network is to define what security means to your organization. A honeypot is just a tool. We have categorized two types of honeypots, production and research. Productions honeypots help reduce risk in an organization. Regardless of what type of honeypot you use, keep in mind the level of interaction. This means that the more your honeypot can do and the more you can learn from it, the more risk that potentially exists. Honeypots will not solve organizations security problems. Only best practices can do that. However, honeypots may be a tool to help contribute to those best practices.

VII. **FUTURE WORK: -** Honeypots are very much useful for the organizations to learn about the black hats both inside and from the external environment. It helps them to know about the attack patterns, their type and the frequency of attacks. Our experiments show that low interaction honeypot can be used as an active defensive tool within an organization to catch the insider threat. High interaction honeypots provide us with a real value data, which is valuable information for the organization if it effectively profiled. This data can be used to increase the network security measures. Researchers focus the two to make honeypot easier to deploy and more difficult to detect. From the advances in research and production honeypot nowadays, we predict the future honeypot has the features of integration, virtualization and distribution. Integrated honeypot encapsulates all the components in a single device. Virtual honeypot creates large number of honeypot systems in one machine. Distributed honeypot comprises different honeypot system in an actual network to offer high interaction between attacks and system. All of them make future honeypot cheaper to apply and easier to maintain.

REFERENCES:-

[1]Xiaoyan Sun, Yang Wang, Jie Ren, Yuefei Zhu and Shengli Liu, "Collecting Internet Malware Based on Client-side Honeypot", 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2012.

[2]C. H. Nick Jap, P. Blanchfield, and K. S. Daniel Su, “The use of honeypot approach in software-based application protection for shareware programs”, IEEE International Conference on Computing & Informatics, (ICOCI '06), pp. 1-7, 2012.

[3] JianBao and Chang-peng Ji, and Mo Gao, “Research on network security of defence based on Honeypot”, IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010.

[4] Anjali Sardana, R. C. Joshi, “Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level”, IEEE International Symposiums on Information Processing (ISIP), pp. 505-509, 2013.

[5] Jones, J.K. and Romney, G.W. Honeynets: An Educational Resource for ITS Security SIGITE '04, Salt Lake City, Utah, 2004.

[6] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Project Using honeypots. *Journal of Computing Sciences in colleges*, *20* (4).