**HONEYPOTS IN NETWORK SECURITY**

**NAME: MUNMUN AKOND**

**ID: 17-33641-1**

**SECTION: A**

**MOTIVATION**

First of all, we are very interested in this subject field of study and we want to work this field it’s kind of interesting for us, it’s related to our daily works. So, we choose this topic and our motivation for this research is to understand how security systems are working and how an organization can be protected and being aware of the risks of security flaws in the system. We will learn how a system is working and how it can be developed. Because, it is easy to hack a system but it is tough to protect a system from the attacker.Nowadays, The internet is well and truly on the rise,there are billion of users in internet. Nearly all of these users have had or will have some form of personal data online, and where there is personal data, there is always somebody trying to gain hold of it. A quick look around any room in a home or business and anybody could pick out a few internet connected devices, many of which don’t have security administrators monitoring them. There are many examples of this happening daily, with malicious attacks.

The motivation for this, to try and develop a Honeypot which can be used by information-security teams that can be used to detect and record an attack while it is happening, while gaining future knowledge on how to prevent such attacks.

With the increasing reliance on technology, it is becoming more and more essential to secure every aspect of online information and data. As the internet grows and computer networks become bigger, data integrity has become one of the most important aspects for organizations to consider. Network security is one of the most important aspects for organizations to consider when working over the internet, LAN or other method no matter how small or big the business is. While there is no network that is immune to attacks, a stable and efficient network security system is essential to protecting client data. Honeypots in network security system helps business reduce the risk of falling victim of data theft and sabotage. In todays digital age, Network security has a demandable side in business-world. Every work-station needs protection from there harmful spyware. At there, Network security is so important. Network security also ensures that shared data is kept secure. Having your network hacked can put you out of business. This typically involves the planting of misleading information into the systems. It is one of the many tactics that hackers use. For this, honeypot implementation is so helpful.

Security experts often use honeypots and honeynets to protect network systems. Honeypot is an outstanding technology that security experts use to tap new hacking techniques from attackers and intruders.Accoring to Spitzner(2002), founder of the Honeynet Project, “a honeynet is security resource whose value lies in being probed, attacked, or compromised”.

Global communication is getting more important every day. At the same time, computer crimes are increasing. It is important to know, what kind of strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather such information is one main goal of a honeypot. Today, the demand for information security analysis is currently on the rise, and if we go for this field we think we can get better knowledge about our thesis part and it will be helpful for our future.

**LITERATURE REVIEW**

**ABSTRACT:**

Computer Network and Internet is growing every day. Computer networks allow communication faster than any other facilities. Also, Information security is a rising concern today in this era of the internet. These networks allow the user to access local and remote database. It is not so easy to protect every system on the network.If we see, In industries, the network and it’s security are important issues, as a breach in the system can cause major problems. So at there Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alerts the administrator about attack. IDS provide solution for large scale industries only. But there is no solution for the small scale industries. So model is proposed for honeypot to solve the problem of small scale industries which is the hybrid structure of Snort, Nmap, Xprobe2, and P0f. This model captures the activities of attackers and maintains a log for all these activities. HoneyPots are fake computer Systems which appears vulnerable to attack though it actually pevents access to valuable sensitive data and administrative controls. A well designed and developed Honeypot provide data to the research community to study issues in network security like Internet worms, Zero-day attacks, spam control, Dos attacks etc. The developed honeypot server application is combined with IDSs to analyze data in real-time and to operate effectively. Moreover, by associating the advantges of low and high-interaction honeypots. In this paper we present a detailed overview on Honeypot technology. The aspects of using honeypoy in education and in hybrid environment with IDS and different types of Honeypots, Honeypot concepts.

***Keywords:*** Intrusion detection and prevention systems (IDS/IPS), Honeypots, Network security, Network traffic visualization.

**Introduction:**

With the rapid development of computer network technology, the Internet has become more and more widely touched by the field, to bring convenience to people at the same time, computer network security issues are increasingly prominent. The computer network is an open network, the network of shared resources in the uncertainty, leading to the computer and the network vulnerable to hackers, computer viruses and other dangerous behaviour attacks, in addition, the openness of the computer network protocol, but also a network security risks of a reason. In order to make people more secure and safe to use the network, the study of computer network security defense measures become particularly important. There are many ways and means to detect cyber-attack, but most of them are passive defense. We need to establish an active defese and now the most representative of a means of active defense detection is the honeypot technology. By using the honeypot technology we can catches the intruder who attempting to hack the data.

An intruder can be defined as somebody wants to break into an existing computer. This identity is popularly termed as a hacker, blackhat or cracker. System administrators now days have to deal with larger number of systems connected to the networks that provide a variety of services. The challenge here is not only to be able to actively monitor all the systems but also be able to react quickly to different events. There also an outsider attack, it is an attack from a person who is not a member of the organization. Usually the intruder is a hacker whose intensions are to cause harm or mischief. We can classify this intruder into two types, one who has something to gain by the intrusion and the other a curious person trying to probe the security of the system. The first type is popularly termed as a “cracker”. Crackers attack web-sites or database servers in an attempt to gain critical information such as credit card or social security information. The second type is the “hacker” who can be further broken down into two types: an extremely intelligent computer knowledgeable person. An intelligent hacker is one who studies protocols and algorithms and tries to detect vulnerabilities in them.

A honeypot is a program, machine, or a system put on a network as bait for attackers. Honeypots can be classified as deception systems. In 2002, Spitzner [1] defined honeypot is “a security resource whose value lies in being probed, attacked or compromised”. Honeypots should not be viewed as a solution to network security, they should be seen as an aid to it.

**SUMMARY OF THE ISSUES:**

In this work, we explored the concept of honeypot, in the field of IDS and prevention and also know how it works for the network security. There are various type of attackers, intruders, intelligent outsider etc who attempt hacking algorithm to access data from the computer. Although honeypot is a way to control this problems but honeypots doesn’t provide any solution to any problem, nor they fix anything, they are just a tool. It depends on the user in which way they use this tool either for good or for bad.

**CONCLUSION:**

In this paper we discuss the concept of honeypots and it’s application and saw how might be useful to the field of network security. Honeypots offer an offensive approach to intrusion detection and prevention. Most importantly, they serve as a learning tool for system administrators. Honeypots are positioned to become an essential tool for defending the corporate enterprise from hacker attacks, it is a way to spy on your enemies, it might even be a form of concealment. Hackers could be misled into thinking they have achieved a corporate network, when in reality they are just kicking around a honey pot, while the real network remains safe and sound. The advantages that honeypots provide to intrusion protection strategies are difficult to ignore. The use of honeypots and related technologies is on the rise. As awarness and interest in honeypots increases so it will use in an organization as a security tool. There is scope for development of honeypot tools which facilities the different aspects of honeypots like logging, tracing back to the source etc.

**REFERENCES:**

[1] Sobh TS. Wire and wireless intrusion detection system: classification, good characteristics

and state of art. Computer Standard Interface 2006; 28(6):670–694.

[2] Intrusion Detection, Honeypots, and incident Handling Resources. Available from: www.

honeypots.net.

[3] Mukherjee, B., L. Heberlein and K. Levitt. "Network Intrusion Detection." IEEE Network

May/Jun 1994: 26-41

[4] 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, 2006.

[5] Chao-Hsi Yeh and Chung-Huang Yang, “Design and Implementation of Honeypot Systems

Based on Open-Source Software”, IEEE International Conference on Intelligence and Security

Informatics (ISI), 265-266, 2008.

[6] Wei Li-feng, Wang Xiao-bin, “Research on Honeypot Information Fusion Based on Game

Theory”, Second IEEE International Conference on Computer Research and Development,

pp. 803 – 806, 2010,

[7] Yun Yang and Jia Mi, “Design and Implementation of Distributed Intrusion Detection System

based on Honeypot”, 2nd IEEE International Conference on Computer Engineering and

Technology (ICCET), vol. 6, pp. V6-260 - V6-263, 2010.

[8] Spitzner, L. 2002. Honeypots: Tracking Hackers. 1st ed. Boston, MA, USA: Addison Wesley.

[9] Aaron Lanoy and Gordon W. Romney, Senior Member, IEEE [2006] A Virtual Honey Net as a

Teaching Resource.

[10] Brian Scottberg et-al. Internet Honeypot: Protection or Entrapment, 2002.

[11] M. Roesch, .Snort: Lightweight Intrusion Detection for Networks. In Proceedings of the

13th Conference on Systems Administration, 1999, pp. 229.238.

[12] V. Paxson, .Bro: A System for Detecting Network Intruders in Real-Time. Computer

Networks (Amsterdam, Netherlands: 1999), vol. 31, no. 23-24, pp. 2435.2463, 1998.

[Online]. Available: http://citeseer.nj.nec.com/article/paxson98bro.html