Assignment No. 5: Study of Honeypot

Name:	**Class:** B.E.	**Division:** A / B/C
Roll No:	**Date of Submission:**	
Marks Obtained: / 10	**Signature of subject teacher:**	

Title: Study of Honeypot

Objectives:

1. To understand issues in cyber-crime and different attacks

Outcomes:

Analyze threats in order to protect or defend it in cyberspace from cyber-attacks.

Theory:

[1] Honeypot:

Honeypot is a computer system. There are files, directories in it just like a real computer. However, the aim of the computer is to attract hackers to fall into it to watch and follow their behavior. So we can define it as a fake system which looks like a real system. They are different than other security systems since they are not only finding one solution to a particular problem, but also they are eligible to apply variety of security problems and finding several approaches for them. For example, they can be used to log malicious activities in a compromised system, they can be also used to learn new threats for users and creating ideas how to get rid of those problems.

[2] Production honeypots

Production honeypots are used to protect the company from attacks, they are implemented inside the production network to improve the overall security. They are capturing a limited amount of information, mostly low interaction honeypots are used. Thus, security administrator watches the hacker's movements carefully and tries to lower the risks that may come from it towards the company. At this point, we will try to discuss and find out the risks of using production honeypots. Because while testing the security of the systems existing in an organization, unexpected actions may happen such as misusing other systems using honeypot features. If the network administrator is not aware of this problem, they put organization in a big trouble. Spitzner L.(2002) claims that it is easier to break the honeypot phases into groups and refers that Bruce Schneier model is good for understanding the honeypots. He groups the security issues into several steps, which are prevention, detection and response.

[3] Prevention

Prevention is the first thing to consider in our security model. As a definition, it means to prevent the hackers to hack the system. So, we will try not to allow them to access the system. There are many ways to do this in security. One can use firewall to control the network traffic and put some rules to block or allow it. Using authentication methods, digital certificates or having strong passwords are the most common and well-knownsecurity prevention techniques. There are also encryption algorithms that encrypt data. It is a good way to use it since it encrypts the messages and make them impossible to read. The relation between using prevention and honeypot can be explained as following. If the hacker understands the company he is trying to hack is using honeypots and they are aware of today's security problems, it will make them think about it. It will be confusing and scary for a hacker. Even if a company uses the methods that we discussed in the first paragraph in order to stay secure, it is still good to have honeypot in an organization since security issues are concerned and handled professionally. As the security is very significant, it is always good to be conscious. There is no tolerance when there is a problem, it can give a lot of damage to any company. Because every company has private and important data, there is a need to protect the data from intruders.

[4] Detection

Detection is the act of detecting any malicious activity in the system. We are assuming that prevention did not work so one way or another, a hacker compromised the system. There are some ways for detecting those attacks. The well-known detection solution is Network Intrusion Detection Systems. This technology will help users to know if the network is compromised, but it will not prevent hackers from attacking the system. For companies, such detection systems are expensive. At this point, honeypots are valuable to monitor the activity.

[5] Response

Last component of Schneider's model is response. At this stage, we are sure that we had been attacked and we will have response to it. This is where our forensic investigation begins. When a hacker compromises the system, he leaves traces behind. With the appropriate tools, we can handle the data in a way that we can have some clues about what happened to the system. It is possible to watch log files and try to investigate what happened. More about forensic tools and how to get valuable information from it will be discussed later.

[6] History of Honeypots

In this part, we will give the history of honeypots so far according to Lance Spitzner (2002): 1990-1991: It is the first time that honeypot studies released by Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening With Berferd). 1997: Deception Toolkit version 0.1 was introducted by Fred Cohen. After Clifford Stoll (The Cuckoo's Egg) and Bill Cheswick (An Evening With Berferd) , Deception Toolkitgave an idea of first honeypot structure. 1998: First commercial honeypot was released which is known as CyberCop Sting. 1998: BackOfficer Friendly honeypot was introduced. It was free and easy to configure. It is working under Windows operating system. Most of the people tried this software and the concept of honeypot became more and more known among people. 1999: After BackOfficer Friendly, people were more into this new technology. Honeynet project started at this year. Also, Know Your Enemy papers were also released. Thanks to these releases, people understood the aim of the honeypots more 2000-2001: Honeypots started to be used for capturing malicious software from internet and being aware of new threats. Companies began to use honeypots in their systems to improve security and see the malicious traffic. 2002: Honeypot concept became popular and honeypots improved their functionalities, so they became more useful and interesting for both researchers and companies.

[7] Advantages of honeypots

There are many security solutions available in the market. Anyone can browse the variety of choices through internet and find the most suitable solution for their needs. Here are the reasons why we should choose honeypots according to Mokube I. and Adams M. (2007): Honeypots can capture attacks and give information about the attack type and if needed, thanks to the logs, it is possible to see additional information about the attack. New attacks can be seen and new security solutions can be created by looking at them. More examinations can be obtained by looking at the type of the malicious behaviors. It helps to understand more attacks that may happen. Honeypots are not bulky in terms of capturing data. They are only dealing with the incoming malicious traffic. Therefore, the information that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the investigation far easier. Therefore, this makes honeypots very useful. For the only malicious traffic, there is no need for huge data storage. There is no need for new technology to maintain. Any computer can be used as a honeypot system. Thus, it does not cost additional budget to create such a system. They are simple to understand, to configure and to install. They do not have complex algorithms. There is no need for updating or changing some things. As honeypots can capture anything malicious, it can also capture new tools for detecting attacks too. It gives more ideas and deepness of the subject proving that it is possible to discover different point of views and apply them for our security solutions.

[8] Disadvantages of honeypots

As there are several important advantages of using honeypots, there are also some disadvantages of them as well. We are continuing with Mokube I. & Adams M. (2007)'s studies:We can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information. If there is an attack occurring in another system, our honeypot will not be able to identify it. So, attacks not towards our honeypot system may damage other systems and cause big problems. There is fingerprinting disadvantage of honeypots. It is easy for an experienced hacker to understand if he is attacking a honeypot system or a real system. Fingerprinting allows us to distinguish between these two. It is a not a wanted result of our experiment. The honeypot may be used as a zombie to reach other systems and compromise them. This can be very dangerous.

Conclusion:

As we all know network security is very significant for all computer systems because any unprotected machine in a network can be compromised in any minute. One may lose all the secret and important data of a company, which can be a great loss, and it is also very dangerous that someone else knows your important personal information. Thus, we tried to find answers for honeypots' security using all interaction honeypots possible.We Studied prevention & detection of Honeypot along with advantages & disadvantages

Lab Exercise:

1. What is a honeypot? How it protects against cyber attacks
2. what is the role of honeypot in network security