Honeypot: Inventiveness Study

Team:

Team Name: Crypto Tech.

Team Member Name: Chiranjib Parida

Abstract:

Day by day, more and more people are using internet all over the world. It is becoming a part of everyone’s life. People are checking their e-mails, surfing over internet, purchasing goods, playing online games, paying bills on the internet etc. However, while performing all these things, how many people know about security? Do they know the risk of being attacked, infecting by malicious software? Even some of the malicious software are spreading over network to create more threats by users. How many users are aware of that their computer may be used as zombie computers to target other victim systems? As technology is growing rapidly, newer attacks are appearing. Security is a key point to get over all these problems. In this thesis, we will make a real life scenario, using honeypots.

Honeypot is a well-designed system that attracts hackers into it. By luring the hacker into the system, it is possible to monitor the processes that are started and running on the system by hacker. In other words, honeypot is a trap machine which looks like a real system in order to attract the attacker. The aim of the honeypot is analyzing, understanding, watching and tracking hacker’s behaviors in order to create more secure systems. Honeypot is great way to improve network security administrators’ knowledge and learn how to get information from a victim system using forensic tools. Honeypot is also very useful for future threats to keep track of new technology attacks.

Keywords: Honeypot, hacking, security, network.

Introduction:

Scale of Internet technology is very large and it is still growing every day. The security of network is required for improvement of the industries which are dependent on the internet to enhance the business and providing services on the network. So security of network is primary concern of the industries for securing the critical information. Big sums of attacks are noticed in recent years on these kinds of industries. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alert the administrator. IDS and firewalls are used for protecting the system and network from attacks, but after so many efforts for security still the network is not fully secured so different types of solutions are proposed by the experts. The small scale industries using LAN have to keep high their own security level as the database, server and clients are all handled by themselves. Since threat from internal network is Always the big challenge for the administrators, so a solution is required for small scale network to secure their internal network. This report provides the solution for the same using honeypot.

System Requirements:

Hardware Requirements:

At least a Pentium II 450 Mhz processor

At least 512MB of RAM

One NIC (supported by the OS)

One hard drive with at least 10GB capacity. Smaller hard drives allow for shorter image creation times.

Software Requirements:

Any Linux Operating System both x86 and x64

Any Linux Compatible IDE

Python Programming Language

Methodology:

In this project, we have installed honeypot in the local machine and the local machine will have connected to a particular network. Then we have assigned the local IP address to the honeypot and also assign a particular port number and given a MOTD after that honeypot will ready to run.

When the attacker click the IP address of the victim machine then the attacker system information will be coming to the hacker machine and save in the local machine .MMH format or save in secure manner.

MMH:

The information should be:

Time: Means when the attacker click the victim IP address that time, date with attacker IP address

Connection: the attacker connection is alive or not

User-Agent: It gives the attacker machine information like web browser agent information etc.

Accept-Encoding: gzip, deflate

Accept-Language: en-IN,en;q=0.9,en-GB;q=0.8,en-US;q=0.7

And this project we have applied the client-server model

Conclusion:

Honeypot is not a solution to network security but a good tool supplements other security technologies to form an alternative active defense system for network security. Working with IDS and firewall, Honeypot provides new way to attacks prevention, detection and reaction. Honeypot can serve as a good deception tool for prevention of product system because of its ability of trapping attacker to a decoy system. Supplemented with IDS, honeypot reduces false positives and false negatives. This kinds of honeypot share the common technologies of data control and data capture. Honeypot easier to deploy and more difficult to detect.

The largest challenges facing the world today is to protecting the servers against the attackers, that is to provide the security to the network, this is done by honeypot indirectly .It provides the resources to gather information about the attacker, but it carries a lot of risk.

Reference:

- Sadasivam K. & Samudrala B. & Yang T.A., 2005. Design of network security projects using honeypots.p.282-291.

- Iyad Kuwatly, Malek Sraj, Zaid Al Masri, and Hassan Artail, “A Dynamic Honeypot Design for Intrusion Detection”, ©2004 IEEE.
- Mueller Patrick and Shipley Greg, “Network Computing”, Aug 2001 http://www.networkcomputing.com/1217/1217f2.html.
- Northcutt Stephen, “Network Intrusion Detection”: An Analysis Handbook. New Riders Publishing, 1999.