Benefits of Honeypots in Education Sector

Ateeq Ahmad [†] Muhammad Ali [†] and Jamshed Mustafa [††],

[†]Faculty of Science Department of Computer Science, Northern Border University, Arar, Saudi Arabia
[††]Department of Electrical Engineering Northern Border University Arar, Saudi Arabi

Summary
Wealth of information elicited from multiple sources and stored in small hard-disk is a wonder of science but the flipside in its susceptibility to hacking; therefore information security is a growing concern today for organizations and individuals alike. Leading to search for aggressive forms of defense and supplement the existing methods. One of the best possibly ensures is Honeypots. Honeypots are a creation of the IT security designed to attract troublemakers lurking about on the Internet. Honeypots used to identify the tools in their toolkit and provide vital information on current security threats, attacker tools, and attacker mentality. The purpose of this Article is to provide awareness in IT students and IT security professionals in terms of real-time security throughout the educational institutes and provides students with real-time security education. Now a day's technology changes rapidly and due to communication delay's the information about current tools in IT education can cause a major detriment to IT education. The research related to honeypot is still underway in the IT security Lab and conclusion of our research is to provide an effective educational resource and tool to help and solve the challenges in IT security education.

Key words:
Honeypot, Benefits, Security Threats, Types of Honeypot, History.

1. Introduction

Computer technology is more and more ubiquitous; the penetration of computer in society is a welcome step towards modernization but society needs to be better equipped to grapple with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficulty for the security professionals in order to catch hackers. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information. The recent research is focused on bringing quality security training combined with rapidly changing technology. But Pakistan sticks to the traditional approach to security have been largely defensive so far, but interest has to be increasingly paid to more aggressive forms of defense. One of these forms is decoy-based intrusion protection through the use of honeypots. It is the most popular way of discovering latest security threats in the corporate world or in education sector.

2. Definition

To misconceptions in terms of the definition some of them think Honeypot is a tool for deception, whereas others consider it a weapon to lure hackers and some of them think it is simply another intrusion detection tool. The following definition is closer to the purpose of this research.

A "Honeypot" is a security resource whose value lies in being probed, attacked, and compromised (L. Spitzner, May 2002).

According to this definition whatever we designated as a honeypot, their purposes are to probed and exploit the system without being care what the resource is (a router, scripts running emulated services or a production system). Now it is clear from the definition that the manifesto of Honeypot is totally different from other Network security tools like firewall. The orthodox technology like firewall was used for blocking outbound and inbound ports in order to secure the network but couldn't able to inform who is trying to intrude into the system. After that Network Intrusion detection (NIDS) and intrusion prevention systems (IPS) were used for security purpose. The role of this security system is to detect as well as prevent system from intruders. Honeypots are different in that they are a highly flexible tool that can be applied to a variety of different situations like it can be used to capture and analyze automated attacks, such as worms, or act as early indication and warning sensors which are also, the characteristics of Intrusion detection systems. Honeypots can also be used with firewall to deter attacks. Honeypots are security resources that have no production value and any activity or traffic sent to the honeypot is most likely a probe, scan, or attack.

3. Objectives

The main purpose of the research paper is to learn the tools and motives involved in computer and network attacks and share the lesson learned with the University student, those who are involved in research related to network security. There is a commitment to moving far

Manuscript received October 5, 2011
Manuscript revised October 20, 2011

beyond theory and providing solid information about common threats in Universities Network infrastructure.

4. History

Though a great deal of research and deployment had occurred within military, government and commercial organizations, public knowledge of honeypot concepts was scant at best before 1990 as Little if any material could be found before 1990 though/nevertheless. The first resource was a book written by Clifford Stoll titled The Cuckoo's Egg. The second is the whitepaper "An evening with berfered in which a Cracker is Lured, Endured, and studied", by the security icon Bill Cheswick. Before 1990 honeypots had developed and used by a variety of commercial organizations.

The book Cuckoo's Egg, written by Clifford Stoll had discussed the series of true events that occurred in Lawrence Berkeley Lab where he worked as an astronomer. One day his administrator asked him to discover 75-cent accounting error infiltrated one of his system by an attacker, code named "Hunter". He spent over ten months to monitor the techniques used by an attacker instead of disabling and locking him out of the system in order to hunt him. Stoll computers were production systems used by the academic and research communities but he used the concept very similar to honeypot technologies.

Stoll book was not technical but the most fascinating thing in his book was his approach to gaining information. In the system of SIDNET, for strategic Defense initiative Network, he creates a bogus directory and filled that directory with interesting files in order to lure attacker. His goal was to identify the motives of an attacker, that's why he filled the directory with the documents those, appeared to have financial value and government secrets. The attacker by passed the financial documents, this indicated that his motives were to gain highly secret information.

Unlike the book, Bill Cheswick's paper "An Evening with berfered in which a Cracker is Lured, Endured, and Studied was more technical, because it was written by security professionals for the security community in 1990. Everything in the Cheswick paper was nonfiction and it was the first documented case of a true honeypot. In the paper, not only he discussed that how the honeypot was built and used but how a Dutch hacker was studied as he attacked and compromised a variety of systems.

His goal was to learn threatening activities happening on his networks and systems, in order to achieve that goal he built a system with several vulnerabilities (including send mail). He created a controlled environment called "jail" where he took us step by step how an intruder (called Burferd) attempted to infiltrated the system. He also explained not only the different methodologies he used in building his system but also how these methodologies were used.

However, neither provides a precise definition of honeypots but both Stoll's book and Cheswick paper make for fascinating reading, for anyone interested in honeypots.

After seven years of The Cuckoo's Egg and "An Evening with Berferd" the first version of public honeypot solution, named Deception Tool Kit (DTK) was released in November 1997, developed by Fred Cohen. It is a first free UNIX based honeypot solution made up of Perl scripts and C code collection. DTK can also emulate a variety of known UNIX vulnerabilities similar like Bill Cheswick's Berferd. The purpose of DTK is not only to log the attacker's behavior and actions and reveal its information but to deceive the attacker.

Next year, in 1998, first commercial honeypot product named, CyberCop Sting, was developed by Alfred Huger at Secure Networks Inc., it was purchased by NAI in 1998. It ran on Windows NT system and not UNIX, that's why several features were different from DTK. It has also the capability to emulate different systems like Cisco router, Solaris server, and an NT system at the same time. CyberCop sting not only has increased the chance of the honeypot being found and attacked but also improved detection of an alerting to the attacker's activity.

CyberCop Sting never really took off as a commercial product and has now been discontinued. After CyberCop Sting several excellent commercial honeypot products have been released like, NetSec's Specter and Resource's Mantrap.

Marty Roesch and his colleagues, in 1998, began work on a honeypot solution for a large government client, while working at GTE Internetworking they developed a honeypot system that would simulate an entire class C network, approximately up to 254 systems, using a single host. It has the capability of emulating seven different kinds of operating systems with the variety of services.

In the same year 1998, Network Flight Recorder released a Windows-and Unix-based honeypot, named BackOfficer Friendly developed by Marcus Ranum. Extremely easy and freely available over internet, all one had to download the tool, and can be installed in any windows based desktop system. BOF was many people's first introduction to the concept of honeypot though limited in its capabilities.

In 1999 a first non-profit research group of 30 security professionals formed a Honeynet project. The purpose of this group is to learn about the techniques and tools used by blackhat community and sharing what they learn. Honeynet is the advanced type of honeypot, used for detecting and learning about attacks and the attackers themselves. The group has released series of paper known as "Know your Enemy", first publicly documented for the security community. After that they released the book

Your Enemy, in 2001 that documented their research and findings.

There was a sudden growth in both Unix-based and Windows-based worms during 2000 and 2001. Obtaining copies of the worm for analysis and understanding was one of the challenges that various security organizations faced because of data pollution or, as in the case of the CodeRed worm, because the worms only resided in the system memory, but honeypot capturing these worms and proved them a powerful solution to the security community.

On June 19, 2001 Sub7 Trojan was detected. The Trojan listened on the default port 27374 and took over the total remote control of windows system. On June 21, Johannes Ulrich of the SANS Institute deployed a honeypot in a windows system infected with Sub7 Trojan. They captured an attack within minutes and provided it to Incident team for analyzing. They discovered the worm was pretending to be a Sub7 client and try to infect the system which was already infected by Sub7 Trojan. Since the systems were already compromised that’s why it saved the trouble of attacker of hacking into the systems. Ryan Russel at securityFocus.com also began using honeypots for capturing worms such as CodeRed II worm for analysis. Awareness and value of honeypot has been developed with these incidents in the security community and security research.

An unknown exploit has been captured by honeypot technologies on January 8, 2002. The CERT Coordinator Center, a security research organization had released an advisory for the CDE Sub process control Service for an exploit, an attack never seen before captured by a Solaris honeypot. An attacker could gain access to any UNIX system running the dtspcd service. CERT was able to release an advisory based on this information, that the dtspcd attack captured by honeypot is being used by blackhat community. According to this incident it has been clear that honeypots are capable of capturing not only known attacks but can also capture unknown attacks such as worms.

Often people cautious regarding honeypots is that there has never been an agreed-upon definition of honeypot. Organizations discussed different definitions or understanding of what honeypot do and how they operate. Some consider they are technologies designed to detect attacks while other consider them a device to lure and deceive attackers. It’s difficult for organizations to adopt a technology why they don’t even understand what it is.

When Marcus Ranum released the TIS Firewall Toolkit in the early 1990s, everybody understands the purpose of the technology is to save the network from bad guys. Firewall and Intrusion detection systems are easier to understand because they are focus on a specific problem. In contrast, honeypots are highly flexible technology but due to some misunderstanding few organizations trust or understand the technology. As of 2002, this cycle is beginning to break. More and more organizations recognizing the value of honeypots and due to which honeypots have a growing and exciting future ahead of them.

5. Types of Honeypot

Generally honeypot can be divided into two categories: production honeypots and research honeypots. The idea comes from Marty Roesch, developer of Snort (Open source rule based Intrusion Prevention System). According to his evaluation during his research in GTE Internetworking production honeypots protect an organization while research honeypots are used to learn.

5.1 Production honeypot

Honeypot Can be implemented in any organization to deal with the bad guys in order to secure their environment. Production honeypots have less risk because of their simplicity and easy configuration. It is because of simplicity production system provide less information which can only deal with the information that from which systems the attackers are coming from and what exploit they launch but cannot be able to learn how they develop their tools and how they communicate among each other.

5.2 Research honeypots

are designed to gain information about, who the attacker are and, how they organized, what kind of tools they obtained in order to attack systems. This kind of honeypot helps organization indirectly from the security threat that’s why often used by universities and military organizations.

5.3 Low-Interaction honeypot

This kind of honeypot can be compared with any passive IDS since it cannot modify network traffic in any way and do not interact with the attacker. However, it can be used to analyze spammers and can also be uses as active countermeasures against worms which can minimizes the risk associated with Honeypots. An example of low-interaction honeypot is honeyd. Honeyd is able to simulate large network structure on a single network host. It works by imitating computers on the unused IP address of a network.

5.4 Medium-Interaction Honeypots

It works similar like Low-interaction honeypots but simulated services are more complicated technically. Medium-interaction honeypots provide the attacker with a better illusion of an operating system since there is more for the attacker to interact with. More complex attacks can therefore be logged and analyzed. Some examples of medium-interaction honeypots include Mwcollect, nepenthes and honeytrap. Mwcollect and nepenthes can be used to collect autonomously spreading malware. These daemons can log automated attacks, and extract information on how to obtain the malware binaries so that they can automatically download the malware. Honeytrap dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks.

5.5 High-interaction honeypots

These are the most advanced honeypots. They are the most complex and time-consuming to design, and involve the highest amount of risk because they involve an actual operating system. The goal of a high-interaction honeypot is to provide the attacker with a real operating system to interact with, where nothing is simulated or restricted. The possibilities for collecting large amounts of information are therefore greater with this type of honeypot, as all actions can be logged and analyzed. Because the attacker has more resources at his disposal, a high interaction honeypot should be constantly monitored to ensure that it does not become a danger or a security hole. A honeynet is an example of a high-interaction honeypot, and it is typically used for research purposes.

6. Benefits of Honeypot

Honeypots have several distinct advantages when compared to the current most commonly used security mechanisms:

6.1 Small Data Sets

Honeypots only pay attention to the traffic that comes to them. They are not concerned with an overload of network traffic or determining whether packets are legitimate or not. Therefore they only collect small amounts of information – there are no

huge data logs or thousands of alerts a day. The data set may be small, but the information is of high value.

6.2 Minimal Resources

Since they only capture bad activity, they require minimal resources. A retired or low end system may be used as a honeypot.

6.3 Simplicity

They are very simple and flexible. There are no complicated algorithms to develop, state tables or signatures to update and maintain. Discovery of new tools and tactics – Honeypots capture anything that is thrown at them, which can include tools and tactics not used previously. Reviewing these advantages show how honeypots add value and can enhance the overall security of your organization.

6.4 Return on investment

Some of the organization thinks that if they deployed firewall now they became secure, but it is there wrong perception because once the organization scrutinized by hacker in terms of firewall or any other encryption and host-based armoring tool hacker will attack with different techniques and tools. In, contrast honeypots quickly and repeatedly demonstrate their value. Whenever any organization attacked by capturing unauthorized activity, honeypots can be used to justify not only their own value but investment in other security resources as well. When management perceives there are no threats, honeypots can effectively prove that a great deal of risk does exist.

7. Conclusion

Although there are risks that arise when deploying a honeypot, the conclusion of this research is that a honeypot can be safely deployed in an educational environment to assist in the learning experience of students. A few years ago, due to resource limitations, risk assessments, and time restrictions, it may have been impractical to deploy a honeypot. However, the risks and time involved with deploying a honeypot are minimal when using current honeypot technology. Thus it is the conclusion of this research that a honeypot can be implemented as part of an IT Security Lab to facilitate a more interactive approach to IT training and security education for both graduate and postgraduate students.

References

[1] L. Spitzner, “Honeypot: Definitions and Values.” http://www.spitzner.net, May 2002

[2] The Honeynet Project http://project.honeynet.org.

[3] The Honeynet Project 2001. Know your Enemy. Boston, Masschusetts: Addison-Wesley. http://project.honeynet.org/book.

[4] CERT Advisory CA-2001-18 Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP) http://www.cert.org/advisories/CA-2001-18.html.

[5] http://www.cert.org/advisories/CA-2002-01.html

[6] http://en.wikipedia.org/wiki/Honeypot_(computing)

[7] http://www.honeyd.org/background.php

[8] Baumann, R. and Plattner, C White Paper: Honeypots, Swiss Federal Institute of Technology. Zurich, 2002.

[9] Sutton Jr., R.E. DTEC 6873 Section 01: How to Build and Use a Honeypot.

[10] Spitzner, L The Honeynet Project: Trapping the Hackers. IEEE Security & Privacy, 1(2). 15-23

Ateeq Ahmad received the Master degree in computer science in year 2003 from India. Currently he is working as a Lecturer in Faculty of Science, department of Computer Science, Northern Border University, Arar - Saudi Arabia. His research interests include Social networks, Computer Network, Network Security.

Muhammad Ali, He did his Masters in Communication Systems & Networks from Mehran University of Engineering & Technology, Sindh, Pakistan in 2007. He has been working as a System Engineer in information communication department of Mehran University from 2004 to 2009. Currently working as a Lecturer in Northern Borders University Saudi Arabia in the department of Computer Science. His area of interests is Network securities, Wireless Networks, Routing protocols.

Jamshed Mustafa received the Master degree in Electrical Engineer from University Of Detroit Mercy, Detroit Michigan USA in 1991. He is working in Northern Border University Saudi Arabia in department of Electrical Engineering as Lecturer. His research interests include Computer networks, Network security and Wireless networks.