Honeynets: An Educational Resource for IT Security

Jeremiah K. Jones
265 CTB Brigham Young University
Provo, UT 84602 USA
1.801.422.1297
jeremiah@jkjonesco.com

Gordon W. Romney
265G CTB Brigham Young University
Provo, UT 84602 USA
1.801.422.1297
gr@byu.edu

ABSTRACT

Similar to the "Tar Baby" from Uncle Remus [1], a Honeynet is a system designed to attract troublemakers lurking about on the Internet. Honeynets are a creation of the IT security world intended to draw the attention of hackers, identify the tools in their toolkit, and learn their modus operandi. Our thesis is that Honeynets can be deployed safely in an educational environment to provide students with real-time security education. Honeynets provide vital information on current security threats, attacker tools, and attacker mentality. When implemented properly, Honeynets can also provide IT students with experience in a wide range of skills, helping to focus those skills on network and information security. Furthermore, the research that comes from Honeynets can be shared with IT security professionals to help raise awareness and increase security throughout the world. In a society where technology changes rapidly, the inability to provide IT students with the most current tools and information can quickly become a major detriment to IT education. Due to communication delays and the difficulty in keeping educators current in technology, IT students often receive outdated information. A Honeynet experiment is underway in the IT Security Lab of a higher education institution focused on educating IT engineers. The conclusion of current research is that Honeynets can indeed be an effective educational resource and tool to help solve the dynamically changing challenges in security education.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General – *data communications, security and protection.*

General Terms

Documentation, Performance, Reliability, Experimentation, Security, Theory, Legal Aspects.

Keywords

Information technology, honeynet, honeypot, curricula, security education, information assurance, IT educational resource, laboratory, security best practices, security system engineer, vulnerability prevention.

1. INTRODUCTION

With the rapid increase of technology throughout the world, there has been an equally rapid increase in the abuse of that technology. Every day, new hacking tools and scripts are used to penetrate and compromise networks and computer systems across the globe. Becoming familiar with these techniques and staying current on how to detect malicious activity is one of the most difficult tasks of a security engineer. Security vulnerabilities are often not discovered until after they have been exploited [2]. This makes it difficult for security professionals to stay ahead of the blackhat (or hacker) community.

This same dilemma exists within the realm of IT education. In fact, the difficulties of staying up-to-date with security issues may be even more of a problem in an educational environment due to the difficulty that confronts educators in obtaining current information. The rigorous and focused schedules of educators, combined with rapidly changing technology, can often hinder the educator's ability to constantly review current information. Bringing quality security training into an educational environment has become the focus of recent research and discussion [3,4,5,6,7,8,9].

In the corporate world, one popular method for discovering the latest security threats is the use of a honeypot or honeynet [10]. The focus of this research has been to extend the use of this technology into an educational environment in order to assess whether or not honeynet technology can benefit IT curriculums and training methodologies. Current research indicates that the use of a honeynet within a closely monitored IT security lab can benefit students being trained as IT security engineers.

1.1 What is a HoneyPot?

The concept of a "honeypot" was developed to help IT professionals learn more about hackers and their techniques. Just as historical honeypots were used to attract bees, a network honeypot is used to attract hackers. Although many definitions for a honeypot exist, the following definition is the one accepted for the purposes of this research: a "honeypot is a security resource whose value lies in being probed, attacked, or compromised" [11]. Thus, it is simply a system or resource that is left open and available to the public so that it might entice a user with malicious intent. This resource can then be monitored to learn things, such as the tools used to gain access to the resource and the tools used after the resource is compromised.

1.2 What is a HoneyNet?

This concept of a honeypot was then further developed into the idea of a “honeynet” [12]. Levine defines a honeynet as “a network, placed behind a reverse firewall that captures all inbound and outbound data” [13]. A honeynet is simply a more complicated arrangement of a honeypot, using one or more honeypots within an entire network that is set up for the sole purpose of monitoring a hacker’s activities. This network is then protected by a honeywall, which acts as a firewall to protect the outside world from attacks emanating from within the honeynet.

Honeynets are becoming a popular tool for use in studying hacker mentality and methodology. This project was initiated to use the Honeynet as an educational tool for use in a university environment, in order to better understand and mitigate malicious attacks. This project will seek to further explain the concept of a honeynet, how one can be deployed, and its usefulness, particularly in an educational environment.

2. EXAMPLES OF HONEYNETS

Although many organizations have successfully deployed honeynets, due to privacy concerns and corporate policies, most of these examples remain ambiguous, and only the data from these systems is published.

During the summer of 2002, Georgia Tech established a honeynet in order to assist in identifying security issues on campus [13]. The honeynet was first established as a single honeypot and then developed into a more complicated honeynet. This honeynet has successfully detected exploits and compromises that may otherwise have gone unnoticed on the Georgia Tech network [13].

Another example is the use of a Microsoft 2000 honeypot to aid in the discovery of automated identity theft systems [14]. This honeypot was able to capture the Internet Relay Chat (IRC) communications used by hackers to validate credit card information of identity theft victims. This helped to bring about an awareness of some of the tools available to hackers seeking to steal a person’s credit card or other personally identifiable information.

In March 2003, a honeypot was deployed at the Azusa Pacific University Honeynet Research Project [15]. This honeypot used a default Windows 2000 server installation without patches or updates. Almost immediately, this system began to be attacked by worms, including the infamous Slammer worm. Several more unsuccessful attacks were made against the honeypot. There were also several successful attacks that included gaining administrative privileges. One of the contributions of this honeynet was that it helped to further expand security awareness of botnets—compromised machines that are joined together through IRC.

Further development of honeynet technology was started in 2003 by Dave Dittrich. Through some collaborative work, a honeywall cd was created that greatly simplifies the deployment of a honeynet by supplying a bootable honeywall system [16]. This cd was also used as part of the research for this paper, but proved to be unsuccessful as of the time this paper was authored.

Although many organizations have successfully deployed honeynets, due to privacy concerns and corporate policies, most of these examples remain ambiguous, and only the data from these systems is published.

3. HONEYNETS IN EDUCATION

While the use of honeynet technology has been increasing in the corporate world, this technology has not yet been widely deployed among educational institutions. Through proper deployment and maintenance, a honeynet can become a valuable resource for security students.

3.1 Security Lab at Brigham Young University

Brigham Young University has implemented a security engineering lab for undergraduate and graduate students [3] called ITSecLab. This lab is designed so students can experiment with a variety of security tools without the risk of damaging production systems. Some of the activities that go on in the lab include security scanning, virus and worm analysis, and DoS creation and prevention. One network of the ITSecLab is set up as an isolated “Sandbox” in order to effectively prevent any malicious activity from leaving the secured network.

The ITSecLab at Brigham Young University supports both undergraduate and graduate IT security education and involves a variety of curriculum approaches that allow security students to gain hands-on experience in dealing with all aspects of IT security and information assurance. As an extension to this lab, it was proposed that a honeynet be deployed within the lab facility to experiment with the use of a honeynet as an educational tool.

3.2 Implementing the HoneyNet

Due to the nature of a honeynet, the approach to its network deployment was quite different than other networks of the ITSecLab. The primary difference was that the honeynet required an external connection to the Internet, in contrast to the Sandbox that is isolated from all other networks. The remainder of this section will outline the deployment requirements of the honeynet.

3.2.1 Intended Purpose

The primary purpose for deploying a honeynet in ITSecLab was to experiment with the use of this technology in an educational environment. Subsequent purposes included evaluating the use of honeynet technology for graduate research, as well as developing a method for contributing to the professional world of IT security.

3.2.2 Benefits

Honeynets have several inherent benefits. Some of the features outlined in [17] are:

- Flexibility – The lack of production services allows for easier maintenance and alteration of system services.
- Availability of data – Many production systems are limited in the data that can be produced due to privacy policies. Honeynets have no such restrictions.
- Performance – Recording additional data will often require additional network components. This could adversely affect network performance.
- Purity of data – A honeynet is not used for production and thus all traffic in and out of the honeynet is suspicious. Production traffic or logging does not need to be filtered from a honeynet’s logs.

Further benefits that have come from this specific deployment are outlined in the following subsections.

3.2.2.1 Increased awareness of current security threats

Although the honeynet initially only ran for several days, the quick infection by several variants of the Welchia worm helped to raise awareness of the magnitude of the current worm outbreak. The alert designed to protect the network from such infections was heightened not only among those involved, but also among other IT professionals employed at the institution.

During the short time the honeynet was running, it was the target for several port and other Internet scans. This helped to show that port scanners are used quite commonly to probe the weaknesses of a system. Knowing this, one can then attempt to find ways of preventing port scanning, or at least limiting a port scanner's ability to probe for weaknesses.

3.2.2.2 In-depth learning experience in network security and operating systems

In order for the students to understand how the honeynet would function on a technical level, several advanced networking concepts needed to be clearly understood. For example, in order to understand the advantage of running the honeywall as a layer two bridge, it was necessary for the students to understand how a bridge operates in a network and what role it plays in transmitting data. Additionally, by understanding the various rules and limits that were placed on the honeywall, the students gained an understanding of how malicious activity can often be recognized automatically based on patterns, algorithms, and thresholds placed on 'normal' usage. Being able to configure rules for identifying hacker activity helped the students to understand how malicious activity differs from legitimate activity on a network.

Furthermore, configuring a honeynet to work in bridged mode (without the aid of the honeywall CD) required advanced configuration of a Linux kernel. Although the current kernel release has built-in features to allow for IP filtering while in bridged mode, the kernel used at the time of the project did not have this feature (Linux Kernel 2.4.26). Thus, it was necessary to apply a patch to the kernel and then recompile the kernel in order to add this functionality into the honeywall. Unfortunately, due to hardware issues, the honeywall was not able to be deployed in bridged mode, but the exercise of compiling and upgrading the kernel was an excellent practical experience for the students involved.

3.2.2.3 A general increase in student motivation towards information and computer security practices

Although the research was not intended to qualitatively measure the interest and motivation of the students, it should at least be mentioned that there was a noticeable increase in interest relating to security when the students became aware of the honeynet project. Presentations were requested in several IT courses (including security and networking courses) concerning the honeynet. Even during installation and configuration, there were several students who became involved with the project without receiving any credit (academic or otherwise) for their efforts. Although this is simply a preliminary observation and not a confirmed result, a future study may be implemented to attempt to measure the affect of the honeynet system on student's interest in IT security.

3.2.3 Securing the HoneyNet

Because the sole purpose of a honeynet is to lure attackers, there are certain risks that need to be addressed before deploying such a system. The three main risks involved with running a honeynet are: laws that restrict monitoring rights, harm to other systems as a result of an attacker's activity on a honeynet, and entrapment [10].

First, there are federal and state laws that prohibit certain types of activity from being monitored. It is not the intent of this research to delve into the legal issues surrounding honeynets, but it is necessary for any operator of such a system to understand the legal ramifications of running a honeynet system. Before deploying a honeynet, one should consult with a lawyer or at least be aware of the laws that relate to honeynets.

Second, as a honeynet is compromised, it is likely that an attacker may attempt to use the system to launch an attack upon another system. Responsibility for damage to another system as a result of a honeynet is likely to fall upon the operator of the honeynet. Therefore, it is of the utmost importance to properly secure the honeynet. For this purpose, it is recommended that a generation II honeynet be deployed as opposed to a generation I honeynet [13]. A GEN II honeynet involves the use of a honeywall that acts as a reverse firewall. The Honeynet Alliance has created a bootable honeywall CD [16] that uses several tools including a specialized firewall script and SnortInline. These tools actively stop malicious traffic based on things such as bandwidth usage, known malicious signatures, and likely attacks (such as DoS). Without including a honeywall as part of the honeynet, one runs the risk of harming a remote system due to the local system's compromise. A honeywall was deployed as a standard element in all phases of this research.

Third, in cases where prosecution is a result of catching a malicious user, it is possible the user will claim they were caught as a result of entrapment. Although this does not put the system operators at risk, it is still an issue closely related with honeynets and should be clearly understood before utilizing such a system.

3.3 Ongoing Case Study

A honeynet system has been deployed in the ITSecLab at Brigham Young University and continues to be part of an ongoing case study on the use of honeynets in IT security education. The project began as a graduate-level project and was then accepted as a basic feature of ITSecLab by contributing to on-going research.

3.3.1 Past Research

The honeynet was originally deployed as a system involving a honeywall and a single Windows 2000 Server honeypot. The project was intended to analyze the ease of deploying a honeypot and not to collect significant data about security. The honeynet was successfully deployed after several weeks of working around outdated hardware and limited resources.

Within hours of the honeynet's deployment, the honeypot was infected with a variant of the Welchia worm. The honeywall helped to protect outside networks by not allowing more than 5 outgoing connections per minute. Although the worm did attempt to scan other networks, rather than thousands of scans per minute, it was limited to only 5, thus greatly reducing the chances of another system being infected. Also, because active logging was enabled on the honeywall, the worm was discovered quickly and was cleaned from the honeypot. Two other variants of the Welchia worm also infected the honeypot.

The honeynet was initially allowed to run for only a few days due to academic scheduling but has subsequently been designed to provide dynamic "attack" data through continuous service.

3.3.2 *Current Research*

The success of the initial project precipitated an interest in the honeynet system and resulted in a proposal to have a honeynet included as part of the ITSecLab Lab. This lab was designed to provide students with resources for learning about all forms of IT security. The proposal to include the honeynet was approved, and the project was revived.

The current implementation of the honeynet involves a honeywall and two honeypot machines. There are two ways of configuring a honeywall. The first is in NAT mode, where the honeywall is visible to the outside world and the honeypot(s) are assigned internal IP addresses. The second method is to put the honeywall in bridged mode. This causes the honeywall to act as a layer two bridge so that each honeypot is still buffered with the protection of the honeywall, but the honeywall is virtually invisible to the outside world.

The current honeywall could not be successfully deployed using the Honeywall CD [16], and was therefore set up manually to run in NAT mode. This makes the honeywall visible to the outside world but still provides the protection of the honeywall system. The honeywall could not be deployed in bridged mode due to complications with outdated hardware and the inability to properly compile the kernel to act as a filtering bridge.

One honeypot is running a default installation of Windows 2000 Server while the other is running a default installation of Linux RedHat 9.0.

Several IT Security students (both graduate and undergraduate) will be frequently monitoring the honeynet to ensure that systems outside the honeynet are not compromised. The honeynet is currently not a part of any standardized curriculum but is available to all of the IT Security students to monitor and learn from the data being collected.

3.3.3 *Future Research*

Plans are in place to upgrade the hardware used to initially deploy the honeynet, so the honeywall can run in bridged mode. This will help to reduce suspicion by making the honeywall virtually invisible to attackers. If attackers cannot "see" the honeywall, they are much less likely to discover the presence of honeynet monitoring technology. Improved monitoring facilities, such as a custom data tracking interface, improved alerting, and remote monitoring capabilities are also planned.

It is also proposed that more honeypots be deployed using a variety of operating systems in order to assess some of the vulnerabilities on each system. A virtual honeynet has also been proposed to utilize fewer physical resources, to assist in capturing data, and to facilitate easy re-imaging of the honeypots. Additionally, following the example of Raynal [18], research into honeypot forensics will be conducted. Presentation of honeynet research was one of the primary areas of focus of the recent 2004 IEEE Information Assurance Conference held at the US Military Academy. Academic research in this dynamically evolving area is just now commencing.

Faculty members also hope that monitoring and testing of the honeynet will become a standard part of the IT Security curriculum. It is proposed that students be assigned one or more hands-on labs that involve the honeynet system. This will help to ensure constant monitoring of the honeynet while also assisting in the education of security engineers. By involving the honeynet in the IT Security curriculum, important security principles will be taught in an interactive way, including, identification of worm/virus signatures, experience with DoS attacks, an understanding of intruder mentality, current security threats and exploits, and knowledge of how the blackhat community interacts.

4. CONCLUSION

Although there are risks that arise when deploying a honeynet, the conclusion of this research is that a honeynet 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 honeynet. However, the risks and time involved with deploying a honeynet are minimal when using current honeynet technology. Thus it is the conclusion of this research that a honeynet can be implemented as part of an IT Security Lab to facilitate a more interactive approach to IT training and security education for both undergraduate and graduate students.

5. ACKNOWLEDGEMENTS

We express our appreciation to the IT professors at Brigham Young University for their support and willingness to share limited resources; and to Brady Stevenson, Nathan Green, and Mac McCallister for their continual assistance.

6. REFERENCES

[1] J. Harris, *Brer Rabbit and the Tar-Baby 1879,* Creation Books, 2000.

[2] F. Zhang, et al., "Honeypot: a Supplemented Active Defense System for Network Security," *Parallel & Distributed Computing Applications and Technologies*, pp 231-235, 2003.

[3] G. Romney, et al., "A Teaching Prototype for Educating IT Security Engineers in Emerging Environments," Presented at the IEEE ITHET 2004 Conference in Istanbul, Turkey, June 2, 2004. Published in IEEE Xplore.

[4] P. Mateti, "A Laboratory-Based Course on Internet Security, *SIGCSE'03*, pp. 252-256, February 2003.

[5] C. LeBlanc and E. Stiller, "Teaching Computer Security at a Small College," *SIGSE'04*, pp. 407-411, March 2004.

[6] E. Crowley, "Information System Security Curricula Development," *CITC4'03*, pp. 249-255, October 2003.

[7] J. Hu, C. Meinel, and M. Schmitt, "Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education," *SIGCSE'04*, pp. 412-416, March 2004.

[8] T.A. Yang, "Computer Security and Impact on Computer Science Education," *JCSC*, vol. 16, pp. 233-246, May 2001.

[9] J.M.D. Hill, C.A. Carver, Jr., J.W. Humphries, and U.W. Pooch, "Using an Isolated Network Laboratory to Teach Advanced Networks and Security," *SIGCSE'01*,pp. 36-40, February 2001.

[10] L. Spitzner, "The Honeynet Project: Trapping the Hackers," *Security and Privacy Magazine, IEEE*, Volume 1, Issue 2, pp 15-23, 2003.

[11] L. Spitzner, "Honeypot: Definitions and values." *http://www.spitzner.net*, May 2002.

[12] Honeynet Project: Know Your Enemy:Honeynets – What a Honeynet is, its value, how it works, and risk/issues involved. http://www.honeynet.org Last Modified: 07 January, 2003.

[13] J. Levine, et al., "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks," *Proceedings of the 2003 IEEE Workshop on Information Assurance,* pp 92-99, June 2003.

[14] B. McCarty, "Automated Identity Theft," *Security and Privacy Magazine, IEEE*, Volume 1, Issue 5, pp 89-92, 2003.

[15] B. McCarty, "Botnets: Big and Bigger," *Security and Privacy Magazine, IEEE*, Volume 1, Issue 4, pp 87-90, 2003.

[16] G. Chamales, "The Honeywall CD-ROM," *Security and Privacy Magazine, IEEE*, Volume 2, Issue 2, pp 77-79, April 2004.

[17] J. Yin, et al., "Intrusion Discovery with Data Mining on Honeynet," *International Conference on Machine Learning and Cybernetics*, Volume 1, pp 41-45, 2003.

[18] F. Raynal, et. Al., "Honeypot Forensics," 2004 IEEE Information Assurance Conference, June 10-11, US Military Academy, West Point, New York