Honeypots – An incentive approach to modern security

Prof. Sowmya CV[1], Akshay Anand[2] ,Muskan[3]

[1] Faculty CSE Department, Sri Krishna Institute of Technology, B'lore-560090, India

[2,3]CSE Department, Sri Krishna Institute of Technology, B'lore-560090, India

ABSTRACT

A honeypot is a non-production system created to engage with cyber attackers and gather information about their tactics and behaviors. Over the past three decades, a tonnes of research has been done in the area of network intrusion detection. It is important to have a clear understanding of what a honeypot should and should not perform before deploying one[2].

Network security is a highly important subject in the modern society As a result, in this essay, we explore the idea of honeypots. A honeypot is a fictitious system used to seduce attackers[3]. A honeypot is only intended to lure intruders and attackers[4].

INTRODUCTION

A honeypot is a sort of cybersecurity tool used to draw attention to and identify attempts at unauthorized network access or harmful activities Typically, the intrusive party is a hacker with malicious intent. We may divide this invader into two groups: those who stand to gain from the breach and those who are merely interested and want to test the system's security. The first kind is referred to as a "cracker" in popular culture. Some may have political motivations when they attempt to alter official websites or interrupt regular service.

.Needless to say the "script kiddie is the most common type of intruder[3]. techniques used by the blackhat community[4].

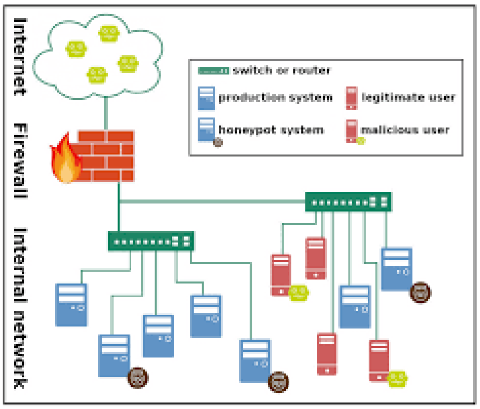
This "script kiddie" is one of the reasons why "security by means of obscurity" will not work. The primary aim of this intruder is to compromise as many systems as possible.. A honeypot is essentially a decoy system that is configured to seem and act like a real target, but it is actually isolated from the rest of the network and is under close security monitoring.

Honeypots are used to gather data about attackers and their strategies as well as to divert their attention away from important network resources. Security experts may learn how attackers try to hack the system, what tools and techniques they employ, and what their ultimate objectives are by setting up a honeypot[1].

One who makes an effort to get access to a working computer is known as an invader. Popular terms for this persona include hacker, blackhat, and cracker. Every day, there are more and more computers connected to networks and the Internet. Intrusion detection has become a difficult task when the rise in networking speed is taken into account[2]. Today's system administrators must manage a greater number of systems that are connected to networks and offer a range of services. The difficulty is in being able to simultaneously actively monitor all the systems and respond promptly to a variety of occurrences. Instances of false negatives. Additionally, these systems offer incredibly little insight into the tools and instructions on what to watch out for. A honeypot's true worth rests in its ability to be probed, scanned, and even hacked. As a result, it should be made available to computers connected to the Internet or at the very least be on par with other computers on the network that one could find on a regular system on a network. These active services are designed to draw the attention of attackers, causing them to invest important time and resources into trying to compromise the system while the attacker is being observed and recorded by the honeypot.

PRODUCTION HONEYPOTS

Organisations use these honeypots as a component of their security architecture. These improve an organization's security measures.



These honeypots may be used to improve security procedures and test intrusion detection systems within an organisation. Production honeypots can send out alerts before a real attack. For instance, a large number of HTTP scans discovered by honeypot is a sign that a new http exploit may be active in the wild. Commercial servers often handle high volumes of traffic, making it difficult for intrusion detection systems to catch all suspicious action. Honeypots can serve as early warning systems and give security managers tips and

display any indicators that it is being watched or that it is a honeypot

BACKGROUND

A honeypot is a programme, machine, or system that is placed on a network to lure attackers in. Honeypots are typically virtual machines that emulate real machines by feigning running services and open ports, services that one might find on a typical machine on a network[5].

RESEARCH HONEYPOTS

As the name implies, researchers or others who are just inquisitive employ these honeypots. These are employed in order to learn more about the techniques employed by the blackhat community. They aid in the development of stronger security technologies and assist security researchers in learning more about attack techniques. They can also assist us in finding flaws in current software or protocols or new attack strategies. Additionally, they can be used to improve or validate current intrusion detection systems. They may offer useful information that can be used in forensic or statistical analysis normally as feasible on the Internet.

SECURITY ISSUES

Honeypots don't offer security to an organisation (they aren't a security technology), but when set up and utilised properly, they improve current security procedures. One may argue that honeypots produce some kind of security risk, which the administrator must manage. Depending on how they are deployed and implemented, there is a security risk. Two perspectives exist about how honeypot systems should manage their security threats.

1. Honeypots that mimic or simulate: There are honeypot programmes that mimic services, vulnerabilities, or both. They trick any attacker into thinking they are gaining access to a specific system or service. Using a tool that is properly designed, you can learn more about a variety of servers and systems.

2. A Honeypots that are actual systems: According to this point of view, since the major goal of honeypots is to safeguard actual systems, they shouldn't be anything other than genuine systems. These honeypots employ genuine systems and servers that are in operation in the real world (SSH), file transfer protocol (FTP), mysql (an open-source database server), and sendmail servers were further installed.

The honeypot shouldn't constitute a threat to other Internet systems, even though we want it to be hacked. Network traffic exiting the honeypot should be controlled and watched in order to do this. The most important component of the entire arrangement is this. While we do want honeypots to be compromised, we don't want to be held responsible for any harm the honeypot may cause to other systems. A honeypot cannot function and succeed without logging. Here, the goal is to entirely hand over control of the system to the attacker while gathering as much data as you can on the methods used to breach the system.

One can also keep track of the actions and occurrences that follow a successful system compromise, although caution should be exercised to avoid endangering other networks or systems. On a honeypot, it is advisable to have several layers of logging. The quality of the analysis will depend on how well the information is acquired. In addition to offering additional information, several layers can aid in connecting and validating information across layers. In situations when the blackhat discovers the honeypot and tries to erase his traces from the logs, even redundant layers might be useful. Ideally, the logs should be examined even more regularly than once per day.

THE WINDOWS HONEYPOT

On the Windows honeypot, Windows Professional was chosen as the operating system. The Windows honeypot was disguised to appear as though it had been set up and left unattended, similar to how the Linux honeypot was. The following setups were made when the most recent Microsoft fixes were installed:

Internet Information Services(IIS): The Windows web server (HTTP), FTP server, and SMTP server are all part of Internet Information Services (IIS). It has seen several assaults over the years, including Code-Red and Nimda27.

Other services: The mysql server package for the Windows system was installed under Other Services. A java-based web server called Apache-Tomcat was set up and configured using the default parameters on port 8080. The remote procedure call, netbios, and other standard Windows services were all left unaltered.

THE LINUX HONEYPOT

This honeypot runs Red Hat (www.redhat.com) with basic configuration plus the services that were desired to be monitored. The idea here was to make the system look like a regular system that has a few servers running but nothing that is being used extensively. Honeypots can also be configured to fake activity in the form of logins, emails etc to make them appear as if they are being used daily.

It was elected to opt for the other option where the system looks like one that has been installed and configured but for the most part left unattended.

The most often used services in the real world include web server (http), ftp, SSH (secure shell), mail server, and database services. The Linux honeypot was chosen as the platform on which to operate these. Since the Apache web server is included with the Redhat Linux distribution and is running on its default port, it was used as the web server. The default configurations and parameters for the web server were used during installation. A java-based web server called Apache-Tomcat was also set up on port 8080 with its out-of-the-box default parameters.

They behave like any honeypot and are incredibly adaptable. They can easily trick any black hats since it will take them enough time to figure out the false system.

HONEYNET

A honeynet is made up of many different honeypots. These are unique networks created to entice attackers. A honeynet's objective is to gather data on harmful behaviour. The researchers later examine this recorded data to get the pertinent information. High interaction honeypots are called honeynets and don't spoof or imitate anything. These honeypots lessen the likelihood that the hacker will be aware that he is on one.

Because of their great risk, these honeypots cannot be placed everywhere. They require a managed setting and administrative experience.

. Almost every imaginable operating system and application may be used in a honeynet . The honeynet's fundamental components are as follows :

- ➔ *Data control is the act of observing and documenting an intruder's nefarious actions.*
- ➔ *Data capture is the control of an attacker's behaviour.*
- ➔ *Data collection is the process of gathering data and conserving it in one place.*
- ➔ *Data analysis is the process of looking into all the data that has been gathered*

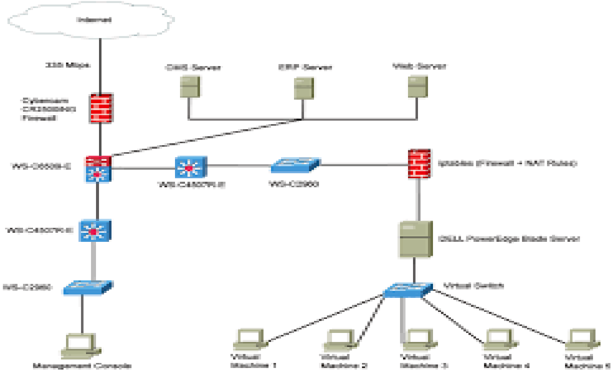


Fig Honeynet architecture

HONEYWALL

One may compare the honeywall to a transparent bridge that prevents malicious data from leaving the honeynet. By doing this, damage to other honeynet systems is avoided. Consequently, honeywall offers data control and monitors outbound traffic.

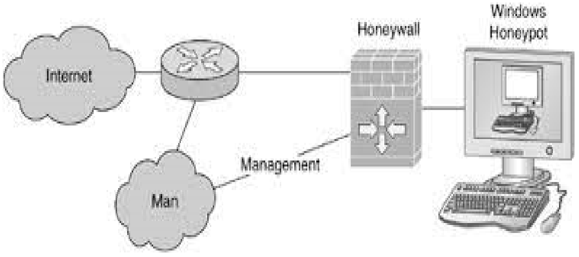


Fig Honeywall

CONCLUSION

A possible instrument in the field of security is the honeypot. When combined with firewalls or intrusion detection systems, they offer an extra benefit. They are adaptable enough to meet our needs and are accessible for both research and commercial use. Various deception techniques, including honey farms, simple port listeners, mobile code throttlers, random servers, and digital breadcrumbs, have used honeypots.

When setting up honeypots, extreme caution must be used because there is a significant amount of risk. Therefore, a thorough risk analysis must be conducted before deployment. Additionally, strict guidelines must be developed for maintenance.

They can extract encrypted data and are Less expensive, adaptable and reliable. Honeypots may be very beneficial if they are utilized in a clever way by using a variety of new technological trends, but laws and legal considerations must be taken into account before they are deployed.

REFERENCES

[1] Mo, Y., Chabukswar, R., Sinopoli, B.: Detecting integrity attacks on SCADA systems. IEEE Trans. Control Syst. Technol. **22**(4), 1396–1407 (2014).

[2] Zhou, C., Huang, S., Xiong, N., et al.: Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Trans. Syst. Man Cyber. Syst. **45**(10), 1345–1360 (2015).

[3] Formby, D., Srinivasan, P., Leonard, A., et al.: Who's in control of your control system? Device finger printing for cyber-physical systems. In: Network and Distributed System Security Symposium (NDSS) (2016).

[4] Pawlick, J., Zhu, Q.: Deception by design: evidence-based signaling games for network defense. In: Workshop on the Economics of Information Security (WEIS) (2015).

[5] Nawrocki, M., Wahlisch, M., Schmidt, T.C., Keil, C., Schonfelder, J.: A survey on honeypot software and data analysis. arXiv preprint (2016)

[6] R. Vishwakarma, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," 2019 3rd Int. Conf. Trends Electron. Informatics, no. Icoei, pp. 1019–1024, 2019.

[7] W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, "BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviours," Inf. Sci. (NY)., vol. 511, pp. 284–296, 2020.

[8] S.T. Park, G. Li, and J.C. Hong, "A study on smart factory-based ambient intelligence contextaware intrusion detection system using machine learning," Journal of Ambient Intelligence and Humanized Computing, vol. 0, no. 0, Springer Berlin Heidelberg, 2018.

[9] D. Wenda and D. Ning, "A honeypot detection method based on characteristic analysis and environment detection," In 2011 International Conference in Electrics, Communication and Automatic Control Proceedings, pp. 201–206, Springer, Berlin, Germany, 2012.

[10] P. Owezarski, "Unsupervised classification and characterization of honeypot attacks," in Proceedings of 10th International Conference on Network and Service Management (CNSM) and Workshop, pp. 10–18, Rio de Janeiro, Brazil, November 2014