DOI : https://dx.doi.org/10.26808/rs.ed.i9v1.03
International Journal of Emerging Trends in Engineering and Development Issue 9, Vol.1 (January 2019)
Available online on http://www.rspublication.com/ijeted/ijeted_index.htm ISSN 2249-6149

A Review-Honeypots on Networks-

Ashutosh Chaudhary
Assistant Professor
Amity School of Engineering & Technology
Amity University Chhattisgarh

Abstract

Cybersecurity is the need of an hour. One of the techniques to ensure this is a honeypot technique. A honeypot is a closely monitored computer resource that imitates activities of production host within a network in order to decoy the attackers. A honeypot is a trap set to detect, deflect or in some manner counteract attempts at illegal use of information systems. In this paper,a detailed analysis of production honeypots and research honeypots isspecified. The widecategorization of honeypots their ideal characteristics, advantages, anddisadvantages are further presented. It also presents the concept of intelligent honeypots.

Introduction-

A honeypot is a computing resource installed in the network in which it is meant to be searched, attacked or compromised by attackers. It is an information resource that is designed to be scanned, attacked andcompromised. By default, a honeypot should have no communication activities towards it. It is a resource that has no production charge. Any interactions spotted on a honeypot will be automatically considered as malicious. The value of a honeypot lies in it being probed, scanned, or compromised. The information taken by the honeypot will be used by network administrators to overcome the attacks be constructed in many forms, either in the form of physical machines, virtual machines (VMs), or emulated virtual hosts. A physical a honeypot is a real computing platform that has its own valid IP address. For example, a computer installed with Fedora Linux or Windows 7 with running network services like FTP, Telnet, or SMTP. A honeypot VM can be built by using virtualization software like VMWare Workstation, QemuKVM, VirtualBox, Parallels Desktop, or User Mode Linux. By using either of these tools, honeypot VM can be twisted with any type of operating system. This software is installed on a computing platform and users can generate single or multiple VMs running on the same host platform. [2],[4].A honeypot can also be built in the form of emulated virtual hosts. By using tools like Honeypot, we can emulate thousands of virtual hosts running different types of operating system on top of a single machine. Each of these virtual hosts is configured with a certain behaviour and personality which defines how the virtual host will respond to attackers' interactions. For example, a virtual host can be programmed to contain a Perl script that is emulating a Sendmail service.There are two types of honeypots: Low -interaction and High-interaction honeypots. The use of the wordinteractionhere means the degree of interaction allowed between the honeypots and the attackers. The level of interaction defines how much damage an attacker can do towards a honeypot.

Types of Honeypot-

Types of Honeypots can be classified based on their purpose and level of interaction.We examine each type in more detail below.

Research Honeypot-

A research honeypot is designed to achieve information about the Blackhat community and does not add any direct value to an organization.Its primary function is to study the way in which the attackers progress and establish their lines of attack, it helps to understand their motives, behaviour and organization Research honeypots are complex to both deploy and maintain and capture extensive amounts of data.Attackers can be observed in action and recorded step by step as they attack and compromise the system. This intelligence assembly is one of the most unique and exciting characteristics of honeypots. It is also a beneficial tool for supporting in the development of analysis and forensic skills. It can even be instrumental in discovering new worms.

Production Honeypot-

Aproduction honeypot is what most people think of when discussing honeypots. A production honeypot is one used within an organization's environment to protect the organization and help mitigate risk., It provides immediate security to a site's production resources. Since they require less functionality than a research honeypot, they are typically easier to build and deploy. Although they identify attack patterns, they give less information about the attackers than research honeypots. You may learn from which system attackers are coming from and what exploits are being launched, but maybe not who they are, how they are organized, or what tools they are using. Production honeypots tend to mirror the production network of the company (or specific services), inviting attackers to interact with them in order to expose the current vulnerabilities of the network. Uncovering these vulnerabilities and alerting administrators of attacks can provide early warning of attacks and help reduce the risk of intrusion [5]. The data provided by the honeypot can be used to build better defences and countermeasures against future threats.

It should be pointed out that as a prevention mechanism, production honeypots have minimal value. Best practices should be implemented involving the use of Firewalls, IDS, and the locking down and patching of systems. The most common attacks are done using scripts and automated tools. Honeypots may not work well against these since these attacks focus on many targets of opportunity, not a single system. Their main benefit is in the area of detection. Due to its simplicity, it addresses the challenges of IDS – there are minimal false positives and false negatives. There are several situations where an IDS may not issue an alert: the attack is too recent for your vendor, the rule matching it caused too many false positives or it's seeing too much traffic and is dropping packets. False Positives occur when an untuned IDS alerts way too much on normal network traffic. These alerts soon get ignored or the rules triggering them are modified, but then real attacks may be missed. In addition, there is a serious problem with the volume of data to analyse with IDS. They can't cope with the network traffic on a large system. Honeypots address these challenges because since honeypots have no production activity, all the traffic sent to a honeypot is almost certainly unauthorized –meaning no false positives, false negatives or large data sets to analyse. Also, once an attack has been detected the machine can be pulled offline and thorough forensics performed something that is often difficult.These categorizations of honeypots are simply a guideline to identify their purpose, the distinction is not absolute. Sometimes the same honeypot may be either a production or research honeypot. It is not as much as how it is built but how it is used.

Level of Interaction-

In addition to being either production or research honeypots, honeypots can also be categorized based on the level of involvement allowed between the intruder and the system.

These categories are low-interaction, medium-interaction and highinteraction. What you want to do with your honeypot will determine the level of interaction that is right for you.

Low-interaction Honeypots-

Low-interaction honeypot has the lowest interaction capability with an attacker and it is also the simplest honeypot to setup. This type of honeypot only provides minimal services and usually, it is in the form of the virtual host with emulated services. For example, a virtual host running an emulated FTP service, built by using honeypot framework software called Honeyd.

Honeyd is a small daemon that has the ability to create and deploy low-interaction virtual honeypots around the network. All these virtual honeypots can be configured to run certain services and the system administrator has the freedom to set the personality of each virtual honeypot

Honeyed is a popular open source low-interaction honeypot framework that offers a simple way to emulate virtual hosts on a single machine [5]. The main advantage of a low-interactionhoneypot is it has a low risk: because it only offers emulated services to the attacker. The attacker's action is limited to what is being offered or emulated within the virtual host, and they can only scan and connect to the offered ports [6]. Another advantage of a low-interaction honeypot is, it is easy to deploy and maintain. Its disadvantage is the amount of information that can be collected by the virtual host is small[1],[2].

Medium-Interaction Honeypots-

Medium-interactionhoneypotislike low-interaction honeypots, they do not have an operating system installed, but the simulated services are more complicated technically Medium-interaction honeypots are slightly more sophisticated than low interaction honeypots but less sophisticated than high interaction honeypots.Although the probability that the attacker will find a security vulnerability increases, it is still unlikely that the system will be compromised[3]. 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 analysed.

High-interaction honeypots-

High Interaction Honeypots make use of the actual vulnerable service or software. High-interaction honeypots are usually complex solutions as they involve real operating systems and applications. In High Interaction Honeypots, nothing is emulated everything is real. High Interaction Honeypots provide a far more detailed picture of how an attack or intrusion progresses or how a particular malware execute in real-time[9]. Since there is no emulated service, High Interaction Honeypots helps in identifying unknown vulnerabilities. But High Interaction Honeypots are more prone to infections and High Interaction Honeypots increases the risk because attackers can use this real honeypot operating systems to attack and compromise production systems.

Other classifications of honeypots-

Besides the level of interactions, honeypots can also be categorized based on their form, i.e., whether they are physical and virtual. For example, a physical honeypot can be deployed as a Windows desktopcomputer with attractive network services such as File Transfer Protocol, Telnet or Simple Mail Transfer Protocol. Since this form of honeypot offers a full suite of an operating system and applications for the attacker to compromise completely, it is usually classified as a high-interaction honeypot[4]. Meanwhile, a virtual honeypot is usually in the

form of a VM or emulation. Honeypots can also beclassified based on their usage: production and research honeypots[6]. A production honeypot is easy to build and deploy because it is simple and requires less functionality. It directly adds value to the security of the organization, aids discovering attacks, and helps to mitigate risks. It gathers less information from the attackers than a research honeypot[7]. Research in this area has resulted in a number of papers discussing specific topics concerning honeypots and how honeypots can be created and deployed[4],[5]. Several papers have explored the use of honeynets as an educational tool for IT students and academic institutions. This research indicates that honeynets can be an effective tool in security education. A significant amount of work is available that details the benefits of honeypots [5].Other papers go into some detail about the strategic considerations involved when using honeypots [5]. There are also papers that describe specific applications of honeypots as building blocks for a system such as a honeycomb, which is used to create intrusion detection signatures [6]. A large amount of helpful information exists on the Honeynet Project at. This website documents lessons learned about security threats through the use of honeypots. Existing work looks at specific areas concerning honeypots; however, it is difficult to find information from a single source that provides an overall picture of honeypots including their benefits, the concepts behind honeypots, the approach to using honeypots, and the challenges involved when implementing honeypots. A research honeypot is very capable of analysing the attackers' tracks in order to extract important information about the attackers' identity, their origins, their tactics, and the tools they use to compromise other systems.

Advantages-

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

• 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[8]. 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.

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

• 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.

Disadvantages-

Honeypots have several risks and disadvantages. Although few in number, it is these disadvantages that prevent honeypots from completely replacing your current security mechanisms.

• Limited Vision – The only activity tracked and captured by a honeypot is when the attacker directly interacts with them. Attacks against other parts of the system will not be captured unless they honeypot is threatened also[10].

• Discovery and Fingerprinting – Fingerprinting is when an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviours. A simple mistake such as a misspelt word in a service emulation can act as a signature for a honeypot.

• Risk of Takeover – If taken over, the honeypot may be used to attack other systems, within or outside the organization. The honeypot could be used to store and distribute contraband.

RELATED WORK-

In this, we are discussing some specific topics concerning honeypots and how honeypots can be created and deployed. Several papers have explored the use of honeynets as an educational tool for IT professional, student and academic institutions [3],[4]. This research indicates that honeynets can be a very effective and powerfultool in cybersecurity education. A significant amount of work is available that details the benefits of honeypots [5], [6]. Some papers go into specific detail about the strategic considerations involved when using honeypots [5]. There are also papers that describe specific applications of honeypots as building blocks for a system such as a honeycomb, intrusion detection signatures are created by honeycomb.Existing work looks at specific areas concerning honeypots; however, it is difficult to find information from a single source that provides an overall picture of honeypots including their benefits, the concepts behind honeypots, the approach to using honeypots, and the challenges involved when implementing honeypots[7],[8]. The purpose of this paper is to do a survey of honeypots and provide a reasonable overview and starting point for persons who are interested in this technology[9],[10].

REFERENCES-

1. Mokube I, Adams M (2007) Honeypots: concepts, approaches, and challenges. In: Proceedings of the 45th Annual Southeast Regional Conference, New York, pp 321–6.
2. Spitzner L (2003) History and Definition of Honeypots, Pearson Education, Boston.
3. Jones, J.K. and Romney, G.W.
4. Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences in Colleges, 20 (4).
5. Martin, W.W. Honeypots and Honeynets – Security through Deception. http://www.sans.org/reading_room/whitepapers/attackin g/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.
6. Harrison, J. Honeypots, the Hottest Thing in Intrusion Detection. http://www.channelinsider.com/article/Honeypots+the+ Hottest+Thing+in+Intrusion+Detection/111384_1.aspx, eWeek Channel Insider, 20TheHoneynet Project, 2004. Know Your Enemy: HoneYlets in.
7. Wagener, G. & Dulaunoy, A (20 11). Adaptive and Selfamfif!.Unable Honeypots.
8. Dionaea http://dionaea.camivore.it/ [10] Jiang, X &llingyan Xu, 2004. BAiT-TRAP: A Catering Honeypot Framework [online]. Available at: http://www. cs. purdue. edulhom es/j in '{X/co lIapsar/public ion s/BaitTrap. pdf
9. TheHoneynet Project, 2004. Know Your Enemy: HoneYlets in Universities [online]. Available at: http://www. honeynet.orglj:lapers/edu/
10. Grimes, R. A., 2005. Honeypotsfor Windows. Berkeley: Apress.
11. AshutoshkumarChoudhary ,Study of Various Routing Protocols in VANET, International Journal of Emerging Trends in Engineering and Development, Issue 8, Vol.1 (January 2018).