International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Honeypots and Its Comparative Study with Intrusion Detection System in Network Security

Sumitra Samal , Yashaswi Vaidya , Sidak Arora
Asst.Professor, Department of Computer Science & Engineering
SSIPMT, CSVTU, Raipur, INDIA
Patra.jyotiprakash@gmail.com
Department of Computer Science and Engineering Raipur, Chhattisgarh
yashaswi.vaidya@ssipmt.com
Department of Computer Science and Engineering Raipur, Chhattisgarh
sidak.arora@ssipmt.com

Abstract- *Achieving the security of network systems is one of the most important and popular technologies in the field of information technology. Network security involves capture, recording and analysis of network events to find out the evidence about the source of the attacks to the system security. Honeypot is the concept that was introduced in the last 10-15 years. It is different from intrusion detection system and firewall. Honeypot is all about creating an artifact that is used to decieve potential intruders and attackers in a neat to protect the system network . Honeypot is an illusive system that is being set for the attackers as a bait to be targeted on. Honeypots are the systems whose value is expected to get probed, attacked or compromised. It is more efficient than than the intrusion detection system or firewalls. Honeypots attract the hackers to expolit vulnerable computer systems that is under observation.*

Keywords- Hoenyd, Honeytokens, IDS, Firewalls, Levels of interaction

1.INTRODUCTION

With the increase in the use of internet, the risks of malicious intrusions are also increasing day by day. It also results in the exploitation of computer networks. The basic security of the information sources are characterized by its access, availability and data integrity. Any disruption of these properties can result in system intrusion and security risks. A good system administrator has a lot of tools in his or her tool kits in order to defeat intruders and hackers from breaking through network workstations. Hackers take advantage of the exploitation of computer network around the world. So in order to protect our production system that contains the real information from the attackers, there is now an e-news called Honeypot which can help you by gathering all the information about hackers. With the increase in the use of global communication , everybody is the target in this era of changing to new operating systems and new applications. Our computer systems are being put on the web & that is making it difficult to try and keep up to all the changes. Honeypots are made for the

attackers to see and them wanting to attack. Implementing honeypots in the network is different from the network system administrator job. Honeypots does not have anything of value. The real information is kept safe in the production system. To gather the strategies of attackers is the primary goal of honeypots. The primary purpose of honeypot is not to be an ambush for black hat community but the focus lies on silent collection of as much information as possible about their patterns, used programs, purpose of attacks. This technology can also be used for the activities like diverting black hats from productive system or catching black hats while conducting an attack.

2.HOW DOES IT WORK?

Honeypot operation includes web trap of attackers who targets operating system services and focus on system brute force and dictionary attacks and analyze data. A secure shell honeypot is deployed using a virtual private server(VPS). Honeyd is a small daemon that creates a virtual host on network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating system. It improves cyber security by providing mechanisms for thread detection amd assessment. Honeyd monitors unused IP space. When an attacker probes an unused IP, honeyd detects the probe, takes over that IP via ARP spoofing, then creates a virtual honeypot for the attacker to interact with. The attacker is fooled into thinking that he is interacting with a successful hacked system[1-4]. In addition , honeyd automatically updates its list of unused IP as systems are added or removed from the network.

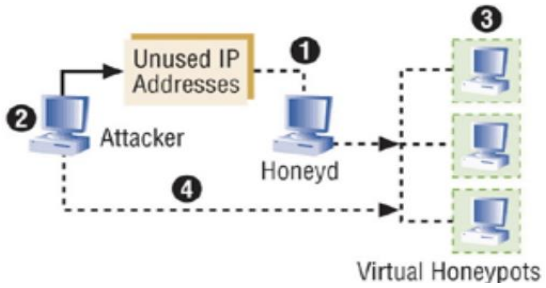

Figure 1-Working of honeypot [3]

3. Architecture of honeypot

The architecture of honeypot within a network mainly comprises of the components that are productions system, honeypots as fake systems and honeynet server. The productions systems are the type of system that imitate the behavior of the real system environment. This allows to know the vulnerabilities of owns system. Research is the type of honeypot which is used understand the motives of the attacker. So honeypots are the set of systems that are in between the real system and the internet.These are the files that are attractive in the perspective of attackers. Honeytokens create the signature that searches for hackers containing key phrases within the document. Logs are maintained in the separate files that stores the information. Also it looks at the access time of the attackers [2].

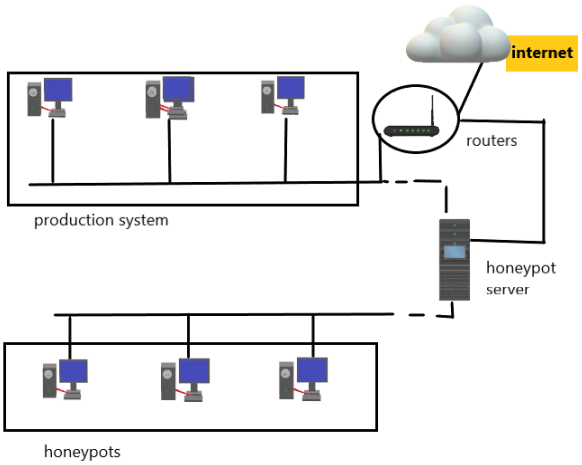

Figure 2 Architecture of honeypot

4. Comparative study of honeypot with other techniques

TABLE 1- Comparison between Firewall and Honeypot

Firewall	Honeypot
It is design to keep intruders out of the network.	It is design to lure intruders to attack on the system.
Only authorized traffic will be allowed to pass.	It allows all traffic to interact with the honeypot system.
Placed at network's traffic entering points.	Placed inside the network as mimic the original production servers.
Logs of incoming and outgoing traffic are maintained, so contains more entries.	Maintain the logs of interacted traffic only, so collect fewer entries.
It cannot protect from internal threats .	It can protect from internal threats.
Firewalls used are packet filter, application level gate-ways, circuit level gateways.	Two types of honeypots are used i.e. production honeypot & research honeypot.

TABLE 2- Comparison between IDS (Intrusion Detection System) and Honeypot [4]

IDS	Honeypot
It monitors the network's traffic and gives alerts to tell about the kind of intruders based upon their database.	It is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information system.
IDS require signatures for detecting malicious	Honeypot does not require any signature for

activities.	detection.
IDS is fail to detect attacks if they are unknown at the time of its deployment.	Honeypot can detect vulnerabilities that are not yet understood or known.
Easy to deploy as it does not affect existing infrastructure.	Deployment complexity is based on type and purpose for which it developed.
It is suffer from the problem of false alerts like false positive and false negative.	It collects information about strategy used and generates alert when intruder try to compromise it, so overcome false alert problem.
According to monitoring scope in terms of area covered, it has two main types Network based IDS, Host based IDS.	According to interaction with intruders it can be divided as low, medium and high interaction honeypots.

5. Types Of Honeypot

Honeypots Are Categorized On The Basis Of The Extent To Which An Attacker Can Interact With The Honeypot And Underlying Operating System. More The Hackers Interact With Honepots, More The Information We Get.

Low-Level Interaction Honeypot System- This Type Of System Are Simple And Easy To Install. It Only Provides Information Of Certain Fake Services. It Involves No Real Operating System That An Attacker Can Operate On. For Example A Simple Netcat-L-P 90>/Log/Honeypot/Port 80.Log Could Be Used To Listen On Port 90(Http) And Log All Incoming Traffic Can Easily Be Recognized And Stored.

Mid-Level Interaction Honeypot- System-It Provides Comparatively More Interaction Services. These Services Are Still Emulated. The Fake Daemons Are More Sophisticated And Have Deeper Knowledge About The Specific Services They Provide.

High-Level Interaction Honeypot System- A High Involvement Honeypot Has A Real Underlying Operating Sysyem. However There Are Higher Risk Involved As It Provides Services Like A Real System. Easier For Hacker To Take Full Control Over It.

6. Advantages Of Honeypots Over Traditional Ids:

1.Small Data- Honeypots Collect Data Only When Someone Is Interacting With Them. Small Data Sets Can Make It Easier And More Cost Effective To Identify And Act On Unauthorised Activity.

2.No False Alerts- Honeypots Sidestep The Problem Of False Positives Because Any Activity With Them Is, By Definition Unauthorized. That Allows Organisations To Reduce, If Not Eliminate, False Alerts.

3.No False Negatives- Again Any Activity With A Honeypot Is Anomalous, Making

New Or Previously Unknown Attacks Stand Out.

4.Resources- Honeypots Require Minimal Resources, Even On Large Networks. According To Lance Spitzner, Founder Of The Honeypot Project, A Single Pentium Computer With128mb Of Ram Can Be Used To Monitor Millions Of Ip Addresses.

5.Encryption- Now A Days, More And More Attackers Are Using Encryption As Well. That Blinds An Ids's Ability To Monitor The Network Traffic. With A Honeypot, It Doesn't Matter If Any Attacker Is Using Encryption; The Activity Will Still Be Captured.

7. Conclusion

The Purpose Of This Paper Was To Define What Honeypot Are And Their Value To Security Community. We Have Described Different Types Of Honeypot And Their Working In This Paper. How Much Activity A Honeypot Allows An Attacker Is Called Interaction. The Value Of These Solutions Is Both For Production Or Research Purposes. Honeypots Can Be Used For Production Purposes By Preventing, Detecting, Or Responding To Attacks. Honeypots Can Also Be Used For Research, Gathering Information On Threats So We Can Understand And Defend Against Them.

8. References

[1]-Https://Www.Youtube.Com

[2]-Https://Krazytech.Com

[3]- Https://Www.Google.Co.In

[4]- Http://Ijettjournal.Org