Review on Honeypot Security

Satish Mahendra Kevat

Student, Department Of MCA, Vivekanand Education Society's Institute of Technology, Maharashtra, India

---

Abstract - *A honeypot is a PC framework that is set up to go about as an imitation to bait cyber attackers, and to recognize, divert or think about endeavors to increase unapproved access to data frameworks. it comprises of a PC, applications, and information that recreate the behavior of a genuine system that appears to be part of a network but is actually isolated and closely observed. All interchanges with a honeypot are viewed as hostile, as there's no explanation behind genuine clients to get to a honeypot. On the off chance that a honeypot is effective, the attacker will have no clue that she/he is being deceived and observed.*

Key Words: Honeypot, IDS, Attack Finder, Deflector, Firewall

1. INTRODUCTION

There has been a significant increase in the number of users that are connecting to the internet day by day, with this increase in user's , the malicious intrusions and risk is also increasing.Various systems are being implemented to detect this intrusions and honeypot is one such intrusion detecting system.
In computer technology, a honeypot is a trap set to recognize, redirect or in some way balance endeavors at unapproved utilization of data frameworks. Its principle point does not include a snare for black hat community but rather the concentration lies in quiet accumulation of data as possible about their pattern, programs utilized and reason for assault. Honeypot creates a log which refers to an intrusive activity by detecting intruders. It also helps to reduce the risks of security breaches.

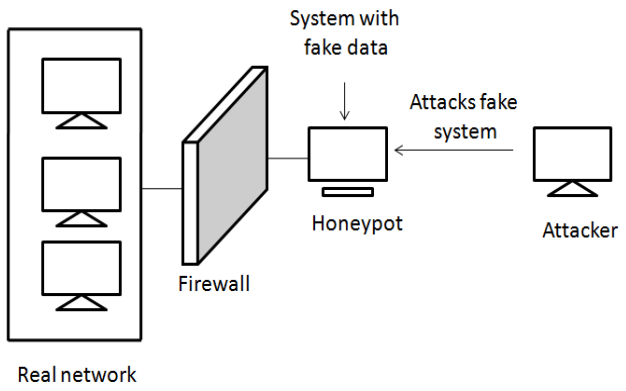

Fig 1: Simple Honeypot

1.1 Where to place honeypot

Honeypots can be placed in any of the three areas in organization; they can be placed externally on the internet or internally on the intranet.

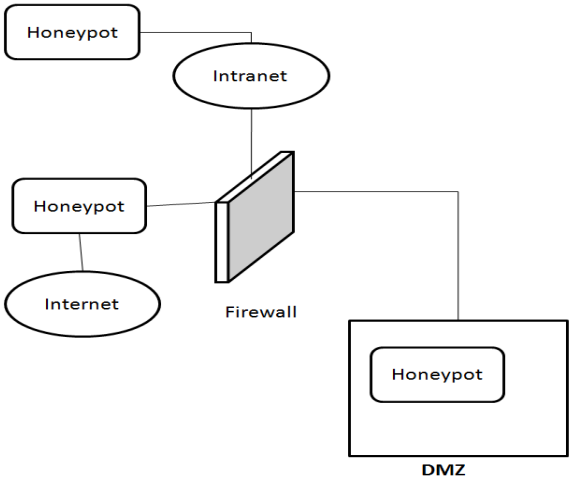

Fig 2: Placement of Honeypot

1.1.1 In front of firewall

When using in front of the firewall (i.e internet), it does not affect internal network, which reduces the risk of compromising the internal system. In this kind of placement, when attacker attacks, the firewall does not create the log and thus, there will be difficulty in locating internal attackers.

1.1.2 Behind the firewall

When using behind the firewall, it keeps the of internal attackers activities and also helps in identifying misconfigured firewall. But being inside the network, some security risks arises, if the internal network is not secured with some additional security mechanism.

1.1.3 DMZ

By placing honeypot inside a DMZ (De militarized zone) itself create a great level of security with flexible environment. But to use in DMZ, it may require some expert knowledge because it involves some complex hardwares.

Thus, honeypot can be placed behind the firewall only if we want to detect the internal attacks or else, it can be placed outside the firewall.

1.2 Building a VM based honeypot

To assemble a honeypot, An arrangement of virtual machines (VMs) are made. They are then setup on a private system with the host OS. To encourage information control, a stateful firewall, for example, IPTables can be utilized to log connections. This firewall would regularly be designed in Layer 2 crossing over mode, rendering it straightforward to the attacker. The last step is information catch, for which tools such as Sebek and Term Log can be utilized. When information has been caught, investigation on the information can be performed utilizing tools such as Honey Inspector, PrivMsg and Sleuth Kit.
This approach is found to be remarkable in its simplicity and feel that a few significant issues need to be brought to light.

1. The choice of a private host-only network. Though this may seem counter intuitive at first, there is a relatively sound reasoning for doing so.

2. While bridging the VMs on to the physical network would seem like a better approach because it transparently forwards packets to the VMs and eliminates an additional layer of routing, it requires an additional data control device which will monitor the packets being sent from the VMs. The operation of data control cannot be performed by the host OS when the VMs are in bridged mode, since all data from the VMs bypass any firewalls or IDSs which exist at the application layer on the host, as shown in the fig 2 below.

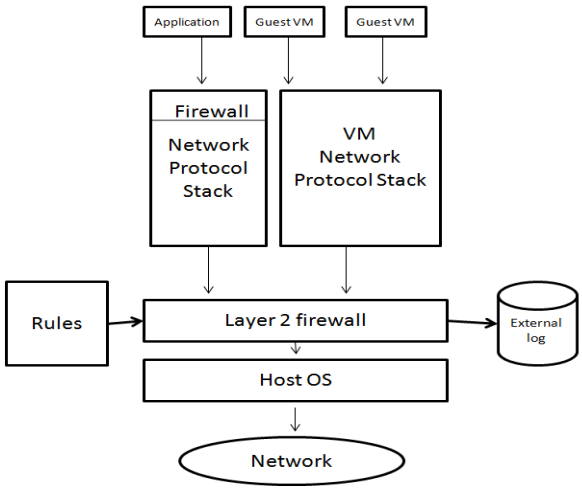

Fig 3: Structure of A VM Based Honeypot

3. The firewall on the host should be transparent to the attacker. This requires considerable effort, since firewalls by default work at Layer 3 or greater.
To render the firewall transparent to the attacker requires recompilation of the kernel. This may not be conceivable on every OS, for example, Windows.
At long last, once a honeypot is breached, a rebuilding component must be implemented with the goal that it is in a split second removed from the system and thoroughly checked before putting it back on the system. This is as of now a manual procedure and can only be partly automated.

2. POINTS TO CONSIDER WHILE IMPLEMENTING A HONEYPOT

2.1 Intent of using:

There are 2 purpose of using honeypot: Early warning and forensic analysis.
Early warning honeypots are easy and simple to setup and are more efficient in catching hackers and malware than other systems. This honeypot helps to detect and identify the attacker with merely a single connection with it.
Forensic analysis honeypot capture and isolate the malware and attacker's tools, and reports the user to create a plan in several days while analysing the attackers captured data.

2.2 Interaction level:

Based on the interaction with the attacker honeypot is named as low, medium and high interaction.
Low interaction honeypot are intended to imitate vulnerable services and identify attacker's assault without uncovering full operating system functionalities.
Medium interaction honeypot are further capable of emulating full services or specific vulnerabilities and may contain basic file structures.
High interaction honeypot mainly emulates the full system and it's capabilities, and are useful for forensic analysis because it may trick the attacker to reveal their more tricks.

2.3 To be deployed on real system or emulation software:

Real systems are best to use because the attacker is having difficulty in differentiating between the genuine system and honeypot. For real systems, old computers can be used. But if we want a low- risk, and quick installation honeypot, emulation software can be used.

2.4 Honeypot administrator:

Honeypot administrator is the person responsible for maintaining the honeypot. This person should install, run, update and maintain the honeypot. If honeypot is not updated and maintained, then it become useless and a jumping off spot for attacker's.

2.5 Updating the data:

If we use high interaction honeypot, it requires continuous updation of data into honeypot , to make it look real. This can be done in some time manually or can be updated using some software or copy programs.

3. Other Security techniques

3.1 Firewall

Firewall defines a single entry/exit point that keeps unapproved clients out of the secured network, denies possibly helpless services from entering or, then again leaving the system and gives security from different sorts of IP mocking and directing assaults.

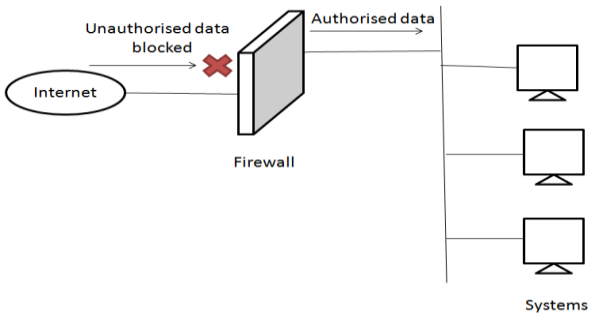

Fig 4: Simple Firewall Deployment

Single gag point rearranges security administration since security abilities are merged on a single system or set of systems. The firewall itself is immune to entrance. This implies that utilization of trusted system withsecure working OS.

A firewall is a collaboration software and hardware which separates an organizations internal network and other networks. Firewalls cannot prevent the attacks from internal system (intranet).

3.2 Intrusion Detection system (IDS)

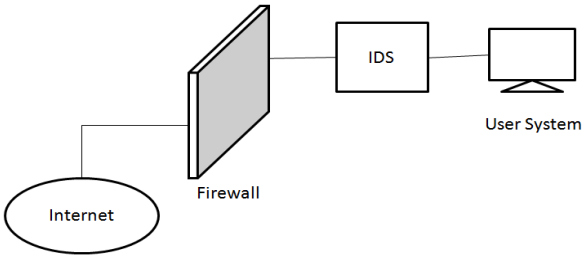

Fig 5 : Simple IDS Deployment

An intrusion detection system (IDS) checks network traffic and searches for any suspicious or irregular activity and alerts the system or system administrator. At times the IDS may likewise react to irregular or malicious activity by making a move, for example, blocking the client or source IP address from getting to the system. IDS are simple to implement as it does not affect existing systems.

Generally, there are 2 types of IDS:

3.2.1 Host IDS (HIDS)

HIDS system runs on the host machine or devices which detect malicious activity on that host. The HIDS monitors the messages/packets and report to the user of any suspicious activity.

3.2.2 Network IDS (NIDS)

NIDS operate on the net- work between the devices. This system monitors the data traffic between this devices in the network for any irregularities or malicious activity. This systems are responsible for monitoring and reporting of entire network rather than a single host.

4. LEGAL ISSUES WITH HONEYPOT

Before using and deploying honeypot, we must understand the legal issues involved with it. The following issues can affect the owner of honeypot:

4.1 Entrapment

Entrapment by definition is “a law enforcement officer’s or government agent’s inducement of a person to commit a crime, by means of fraud or undue persuasion, in an attempt to bring a criminal prosecution against that person”.

Entrapment is only a legal defense and not something that you can sue someone for. This means that, it is used y defendent to avoid conviction. The entrapment issue emerges with honeypots on the grounds that the honeypot os to draw in attackers. This is similar to law enforcement using undercover agents taking on the appearance of drug dealers to attract and catch drug users. There are some huge differences however. There is no recruitment of individuals to interface with honeypot nor is there any connection with the clients that are co-operating with the honeypot. As there are no interaction with individual, it makes the defense of entrapment hard to set up.

4.2 Privacy

The issue revolving around privacy can be complicated. Privacy concentrates on the confidentiality of data. At the point when a network operator monitors the utilization of the system, the users fundamentally lose some measure of privacy.

There are two types of information to track, operational data and transactional data. Operational data includes such things as the address of the user, header information, etc, while the transactional data includes such information key strokes, pages visited, information downloaded, chat records, emails, etc. Most operational data is safe to track without the threat of privacy concerns as there are several different systems out there that track this information already such as IDS systems, routers, and firewalls. The major concern is the transactional data. The obvious comparison is to the phone company. The phone company has every right to privately

track what phone calls you make and for how long; however, it would be illegal for them, without a federal warrant, to listen to or tape your phone conversation. The more content a honeypot tracks, the more privacy concerns are generated.

4.3 Liability

Another legal issue relative to honeypots is the liability. If a honeypot is breached and then is used to attack the systems of another organization, then that honeypot operator could be held liable in a suit brought by downstream victims. Although the harm was inflicted by the intruder rather than the operator, if the honeypot had been secure, then the intruder would not have been able to use it to inflict damage on others.

There are a few steps an organization can consider to reduce the risk. The objective is to make it as troublesome as possible for an attacker to utilize your resources to hurt different systems. Similarly as in Privacy, honeypots have distinctive levels of risk. Low-interaction honeypots have far less risk, as they don't give attacker a genuine working system to interact with. Rather, they control the actions of attackers using emulated services. High-interaction honeypots, are different, they give real working system to attacker to communicate with. Subsequently, most high-communication honeypots have more serious risk.

5. HONEYNET

A honeynet is a system set up with deliberate vulnerabilities; its motivation is to welcome assault, so that an attacker's exercises and strategies can be considered and that data used to build arrange security. A honeynet contains at least one honeypots, which are PC frameworks on the Internet explicitly set up to draw in and "trap" individuals who endeavor to infiltrate other individuals' PC frameworks. In spite of the fact that the main role of a honeynet is to assemble data about attacker's strategies and intentions, the fake system can profit its administrator in different courses, for instance by occupying assailants from a genuine system and its assets.

In addition to the honey pots, a honeynet has genuine applications and services with the goal that it appears like a typical system and an advantageous target.

The Honeynet Project, a non-benefit organization committed to PC security and data sharing, effectively promotes the deployment of honeynets. The association keeps on being on the bleeding edge of security research by attempting to dissect the most recent assaults and instructing people in general about dangers to data frameworks over the world. Established in 1999, The Honeynet Project has added to battle against malware and malignant hacking assaults and has grown to include 30 members of the security community from Canada, Israel, Netherlands, Germany, Australia, and United States.

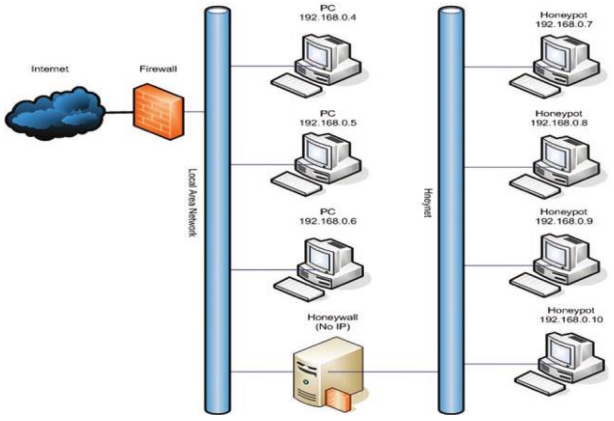

Fig 6: Honey net setup with four honeypots & honey wall

6. CONCLUSIONS

Over the Past few years, the need to improve the network security has arised. To achieve this security, honeypots can be used. They are extremely useful as countermeasures from intruders attacks on systems.So that, the security professionals and researchers can know the person with whom they are and insure the network security is always achieved with the rapid changes in network attacks.

But if the attackers knows about such system or bypasses it then, the whole mechanism is meaningless. Therefore, this fact need to be considered and develop a honeypot in such a way that attacker will definitely believe that it is a original system and not a trap.

REFERENCES

[1] L. Spitzner, "Honeypots: Tracking Hackers",2002
[2] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing)
[3] Navneet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", Vol. 5 (5), 6098-6101, 2014
[4] Aaditya Jain, Dr. Bala Buksh, "Advance Trends in Network Security with Honeypot and its Comparative Study with other Techniques", V29(6),304-312 November 2015
[5] Sandeep Chaware, "Banking Security using Honeypot", IJSIA Vol. 5, No.1, 2011
[6] The Honeynet Project, https://www.honeynet.org/about
[7] Aaditya Jain , Bhuwnesh Sharma , Pawan Gupta, "Honeypot: An External Layer Of Security Against Advance Attacks On Network", IJIRSE,Vol. No.2, Issue 04, April 2016
[8] Honeypot System, https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9
[9] https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide
[10] Muhammet Baykara, Resul Daş, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", Volume 2, Issue 5, September – October 2015
[11] Abhilash Verma, "Production Honeypots: An Organization's view", October 2003