Honeypots: A Boon to Network Security

Priyanka Walavalkar, Huzaifa Momin

Abstract— **Nowadays Computer Networks and Internet has become very significant since it satisfies people with varying needs by providing variety of proper services. Online bills, shopping, transactions and many other essential activities performed on the go by just a single click from our homes.**
It is a boon in this era; it also has its own risks and insecurity too. More efforts should be taken by industries to provide security to their networks and indeed not possible to offer a cent per cent security due to the intangible intelligence of hackers intruding into the network.
This paper exploits the concept of honeypots for providing security to networks of industries which may not have custom intrusion detection systems or firewalls. This proposed paper extracts the various techniques used by hackers and creates a log of all hacker activities.
Thus using this log, attackers can be prevented from hacking the production network system.

Index Terms— **Honeypot, Honeynet, Network, Intrusion**

I. INTRODUCTION

Internet is wide web of network which uses concept of packet switching. The services provided by internet are used by each and every person and hence has greater chances of getting attacked.
Many attacks on Internet are being identified. Some common types of internet attacks are modification of data, spoofing of Identity, password hacking attacks and denial of service attacks.
To overcome all these types of attacks an organization usually installs an intrusion detection system to protect the confidential data exchanged over its network.
There are three main goals of information security namely

- Confidentiality of Data.
- Integrity of data.
- Availability of data.
- **Data confidentiality** ensures that the secure data can be accessed only by authorized persons.
- **Data integrity** allows secure modification of data.
- **Data availability** ensures that the data is available readily to persons who have authority.
- Honeypots and Honeynets are an efficient alternative for such organizations.
- It attracts the hackers to try hacking it which in turn may log the techniques used by the hackers. Logs are useful to prevent such attacks to the legitimate network.
- Honeypot computer usually do not have any important data or information to be secured.
- It only has fake services running on its ports to attract the attackers.
- There are many types of honeypots based on their deployment and design. But Two main types of Honeypots are-
- Production honeypots.
- Research honeypots.
- **Production honeypots** are easy to deploy in the live environment that may capture only some amount of information about the attacks.
- **Research honeypot** deployment is complicated and used mainly for research purposed by government organizations.
- On the basis of design, honeypots can be divided into

1. Shadow Honeypots.
2. Honeynets.
3. Honeyfarms.
4. Honeytokens

A **Shadow honeypot** is a mixture of both honeypot and anomaly detection which is any behavior on the network which is not considered as 'normal' or is characterized as suspicious according to a set of pre-defined rules. At a high level, we use a variety of anomaly detectors to monitor all traffic to a protected network. The traffic that is defined anomalous is processed by a ``shadow honeypot'' to determine the accuracy of the anomaly detection. This shadow is a reference of the secured software that shares all internal state with a regular (``production'') instance of the application, and is supposed to identify possible attacks. Attacks against the shadow are tracked and trapped, and any internal state changes are eliminated. The legitimate traffic that was not classified will be validated by the shadow and will be handled correctly by the system transparently to the user. The result of processing a request by the shadow is used to filter future attack instances and could be used to update the anomaly detector.
A **Honeynet** is a network set up with intentional vulnerabilities; its purpose is to attract attack, so that an intruder's tactics and methods can be studied and that information used to increase network security. A Honeynet contains group of honey pots, which are computer systems connected to Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Since the main purpose of a Honeynet is to gather information about attackers' techniques and motives, this decoy network can profit its operator in other ways, for example by diverting intruders from a real network and its resources.
Honeyfarm as a dedicated set of Honeynet (i.e. high interaction honeypots sitting on a network segment

Manuscript received June 01, 2015
Priyanka Walavalkar, Master of Computer Application, IMCOST, Mumbai University, Mumbai, India
Huzaifa Momin, Master of Computer Application, IMCOST, Mumbai University, Mumbai, India

implemented in such a fashion as to appear to be a functional computing unit comprising different types of machines with various purposes and weaknesses. The notion behind implementing a group of machines is that as opposed to a one dimensional view of an attacker gained from a Honeynet, the defender is able to gain a broader view both of attack behavior and identification of anomalous interactions between different systems.

In the field of network security, **Honeytokens** are honeypots that are not computer systems. Their benefit does not lie in their use, but in their abuse. They are a generalization of such ideas as the honeypot and the canary values often used in stack protection methods. Honeytokens appears in any form, from fake account to a database entry that would only be selected by harmful queries, making the concept almost suited to ensuring data integrity—any use of them is inherently suspicious if not necessarily malicious. They don't always prevent any tampering with the data, but informs the administrator a further measure of confidence in the data integrity. A good example of a Honeytokens is a false email address used to track if a mailing list has been stolen

II. PROPOSED WORK

We have used the concept of honeypots for providing security against attackers. A honeypot computer is set up to act as an easily attacked prey than true or genuine systems. There are two goals for setting up a honeypot.

From the logged information learn how the attackers probe into the network.

Collect appropriate evidences for intrusions of the attackers to submit to law enforcement officers for legal action.

To achieve these goals, the honeypot systems should satisfy certain conditions.

1. The honeypot computer should be similar to other production systems.
2. Usage of interesting information in honeypots to attract hackers.
3. Restrict the traffic sent out to the Internet by an intruder.

Levels of Tracking

Hackers' information retrieved depends on the level of tracking set during setup. It may include firewall logs, system logs and sniffer tools.

Firewall logs

Setting up a firewall into a network is always very useful in addition to honeypot system. It helps in identifying the methods used by an intruder to penetrate into a honeypot computer. Firewalls have different notification capabilities like sms, pager etc.

System Logs

Windows and UNIX are majority operating systems used in Internet and supports logging feature. In Windows, Event Viewer is a tool which provides security by logging the events details. The User Manager provides user management and services run are captured using netsvc.exe. In UNIX, utmp, wtmp, btmp, lastlog are the user activity logs and Syslogd is a log to a remote server.

Sniffer Tools

These tools capture the packets that are flown between honeypot computer and the firewall. Sniffer tools collect more detailed information about intruders when compared to the system and firewall logs. They also offer storage of logs.

Building a Honeypot

Depending on the operating system the tools to be used for building a honeypot varies.

Major Pre-requisites

Computer or Workstation.

Operating system (either Microsoft NT or RedHat)

There are many money-making honeypots readily available in the market namely Tripwire, Cybercop sting etc.

These can be purchased from the market and installed into the local network.

We have implemented the honeypot for capturing hacker information like social security number and ip address.

In a honeypot computer, a fake banking website is made available

A login page is displayed which requires the login id as the social security number and a password to enter into the bank network.

Suppose a hacker tries to intrude into the bank network by providing wrong information or use sql injection techniques a log is captured for the provided details.

The honeypot allows the hackers to enter into the login page as if his login details were validated and displays the page for doing fund transfer which is ultimately a fake page and thereby no harm can be done to the bank.

By this way, a honeypot can be used to capture hacker information intruding into a local network used by small scale industries.

III. ADVANTAGES AND DISADVANTAGES OF HONEYPOT IN NETWORKING

ADVANTAGES

Data Value: All data collected within the honeypot is by definition valuable as there should be no reasonable reason for external persons to access this system.

Resources Utilized: A honeypot uses less resources as the attacker is not trying to flood the system to attempt to achieve access into it, he is attempting to expose specific parts of it to scrutiny. As such there is much less chance of the ‘resource exhaustion’ that an exploit such as a Denial of Service attack would bring.

Simplicity: Intrusion Detection and Prevention Systems and other active security frameworks need to be constantly updated. The Honeypot does not as it is left in its original state until it has served its purpose.

DISADVANTAGES

Fingerprinting: While a honeypot can be used to identify attacks there is a corresponding risk that honeypots can be identified by how they respond to specific types of attacks – this response is known as a signature or a fingerprint.. This let the attacker know that the system is not a valid production system.

Narrow field of view: A honeypot can only provide value if an attack is launched against it. If it has been fingerprinted as a honeypot then would be attackers will bypass it and search for other targets on the network.

Risk: Finally, high interaction honeypots can be used as a springboard for attacks on other systems both inside and outside the boundaries of the honeypot’s network. This may expose the person or company implementing the honeypot to

legal risk if information is stolen from these systems based on weaknesses in the honeypot implementation.

IV. HONEYPOT AS IN WIRELESS AND NETWORK

Interactions levels in honeypots

As we have seen honeypots advantages and disadvantages, now it is time to look into more details in way of levels of interactions. Level of interaction stands for how much the hacker will be able to interact with the system. More amounts of data we would like to gather require more level of interaction. More level of interaction brings more risks into the network security as well. Based on the needs and the purpose of the experiment that one would like to examine, there are three categories of levels of interactions in honeypots. They are low interaction honeypot, medium interaction honeypot and high interaction honeypot. Let us have a look at each of them and compare them one by one:

With **low interaction honeypots**, one can get the least amount of data compared to other honeypot systems. They are limited, so the risk that was taken from intruder is not big either proportionally. First of all, there is no operating system to deal with. They can be used to identify new worms or viruses and analyzing the traffic that is going on through network. Low level of interaction honeypots are easy to configure and understand. In our thesis, firstly we will understand the logic of this category and test how efficient they are.
Therefore, we will start our experiment using the most common low level of interaction honeypot, which is Honeyd. Its last version (1.5c) has been released on 2007.

Medium interaction honeypots are more advanced than low interaction honeypots. Still, operating system does not exist. But this time, more information and more complicated attacks from the hacker can be obtained. As it is more advanced, it has more security holes so that hacker can access the system. Mwcollect, honeytrap and Nepenthes are some of the medium interaction honeypots that are used today.

High interaction honeypots are the most advanced honeypots. Unlike low interaction and medium interaction honeypots, there is an operating system. As a consequence, the hacker can perform anything. Proportionally, more data can be captured from the hacker's activities. However, it is the most risky one when it comes to security as it provides such an access to the hacker that he does not have any restrictions. These kind of honeypots are very time consuming and difficult to maintain. Honeywall is a good example of a high interaction honeypot. We will come back to these security issues covering all these kind of honeypots and discuss and state the exact security problems and come up with some ideas to improve security thanks to our laboratory work.

Wireless Honeypots

In this part, we looked into a different kind of honeypot systems which are wireless honeypots. The goal of deploying wireless honeypots is to capture behaviors of our system in a wireless area and obtain some information and statistics. IEEE 802.11 technology is covered, and also other technologies are possible such as Bluetooth.

Why Wi-Fi Honeypots?

This Wi-Fi structure can be obtained with some access points, wired network and some open-to-attack computers. Wi-Fi honeypots are used to capture unauthorized traffic, and tries to answer questions if it is possible to catch wardriving and hackers which are trying to compromise wireless networks.

Wireless Honeypot History

First idea of wireless honeypots was released by Kevin Poulsen in 2002. During his experiments, he realized that networks are not secure and protected. Intruders are trying to monitor your system, eavesdropping, hacking your system through your wireless network.
Therefore, The Wireless Information Security Experiment started the work in 2002 in Washington USA. After that, the leader of this foundation Rob Lee continued the experiments and tried to answer questions related to wireless hacking, and understand the hackers' ideas and tools, especially the logic behind it.

Late 2002, Tenebris organization in Canada did the monitoring for malicious activities, and understood that there was a huge malicious traffic going on through the network. They did the experiment using wireless honeypot. After that other experiments followed this idea in 2003, 2004 and 2005.All the experiments proved that there had been always threats on wireless networks at that time. Moreover, those kinds of threats still exist today.

In 2004, Laurent Oudot published "Wireless Honeypot Countermeasures" article about wireless honeypots. This article explains the wireless honeypots in detail, its aim and restrictions.

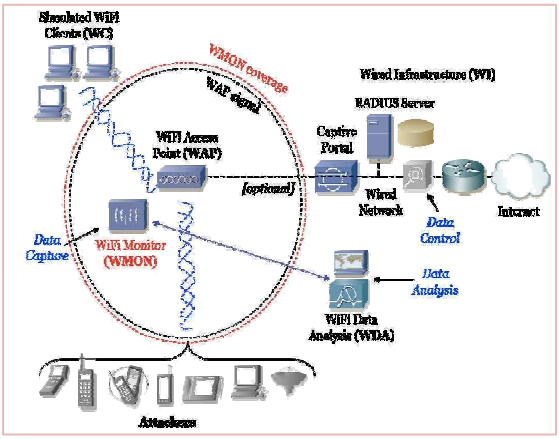
In 2006, a new project was born named MAP Project.MAP was symbolizing the triple suggestions for wireless honeypots: Measure, Analyze and Protect. In this project, hacker was allowed to compromise the system and after that the project members were capturing the malicious activities on the wireless honeypot. However, this project was not improved and it could not answer further questions about wireless honeypots and intruders.

In 2007, "The Hive" project started to answer questions at University of Florida in USA.
Project members tried to discover the attacks' identity, and get additional information about it.

Honeyspot

Honeyspot is the well-known wireless honeypot project supported by Spanish Honeynet Project. The term comes from honeypot and hotspot. Basically, honeyspot was created to watch the hacker and his attacks towards the wireless network. Thus, the traffic that is through the honeyspot is considered as malicious. However, like any other honeypot structures, professional hackers may understand that it is not a real system. So, honeyspot should look as real as possible for the best results. Honeyspot team would like to know the attack type, intruder's ideas, tools, logic, and his approaches. It is very beneficial to get as many information as possible to identify the attack and help to understand any other further attacks in the future. From all these information, honeyspot can answer the questions about the security flaws in WEP

wireless connections and attacks targeted to it. IP address spoofing, web session hacking, MAC address spoofing can be identified. It can also answer the special approaches to hack wireless clients. Thanks to all these information, more secure systems can be created.



The above figure shows the architecture used in honeyspot.WAP which is in the middle is the wireless access point. It gives the wireless networks to the users for internet connection. Attacker can connect to it.

WC (Wireless Client) is the devices that are able to connect to the honeyspot network.
The purpose of this is to create a traffic that is flooding through the network. It is to show the attacker that there is traffic. The real traffic makes sense for the attacker as it looks like a real system. Furthermore, attacker can attack on this stage by using his monitoring tools.

WMON is wireless monitor module. This module captures the traffic in order to have the network traffic information. It helps to understand the attacks, so this module is quite significant at this point.

WDA is wireless data analysis module. This module works with WMON as a team. As WMON is supposed to capture the traffic, there must be a module which is responsible for examining it. Therefore, WMON has the records and saves them in order to send them to WDA for obtaining the information.

WI module is wired structure and it is up us whether to put it in the structure or not. If you wish to create a wired network in your structure, it is also possible. So, WI module gives you a different aspect to your structure.

CONCLUSION

Honeypots are being widely used in network security since longtime. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site, where real resources of information are accessible. The honeypots can also be extended to honeynets, where attacker deals with the multiple honeypots. Using these honeypots and Honeynets the log files analyzed through them can be used to enhance the Intrusion detection system to make it smarter in catching intrusions.

REFERENCES

[1] Spitzner, L. Open Source Honeypots: Learning with honeyd, SecurityFocus, 2003.
[2] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).
[3] Karthik, S., Samudrala, B. and Yang, A.T. Design of NetworkSecurity Projects Using Honeypots. Journal of Computing Sciences in Colleges, 2004.
[4] Know your enemy Honeynets,http://www.honeynet.org/papers/key.htmlSANS institute GIEC certification GSECAssignments#1.4:Honeypots Stretegic Considerations,2002.
[5] Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion Detection Signatures Using Honeypots Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston, 2003,51-56.
[6] Martin, W.W. Honeypots and Honeynets – Security through Deception. http://www.sans.org/reading_room/whitepapers/attacking/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room.
[7] John Carroll, Computer Security, 3rd ed., Butterworth-Heinemann,1997.
[8] Provos, Honeypot Background.http://www.honeyd.org/background.php.