Honeypot: A Security Tool in Intrusion Detection

Er. Sheilly Padda, Er. Sonali Gupta, Er. Apoorva, Er. Lofty, Er. Amandeep Kaur

Computer Science & Department, CEC Landran, Mohali, India

Abstract*—*This paper discusses about the honeypot, which serves as advanced security tool minimizing the risks from attack on IT and networks. The methods deployed to show the working of honeypots are discussed in this paper along with advantage and disadvantages of honeypot.

Keywords—Honeypot, Intrusion, Honeyfarm.

I. INTRODUCTION

Today, Honeypots are still in their infancy, developed and used primarily by researchers and security personnel's. A handful of commercial products are available, and organizations are beginning to deploy open-source honeypots and their more robust iterations, such as Honeyed. But honeypots are not widely deployed.

It is said that "In the near future, honeypots will "learn" your network on their own and dynamically configure themselves". Yet, honey pot technology is moving ahead rapidly, and, in a year or two, honeypots will be hard to ignore. New developments will advance the lab technology with the catchy name to a full-fledged, enterprise-level security tool.

Honey Pot Systems are defined as trap servers or systems, setup to gather information regarding an attacker or intruder into your system. Honeypots can be termed as additional internet security systems and they are an additional level or system. Honey Pots can be setup inside, outside or in the DMZ (*demilitarized zone)* of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes [1]. Honeypots are variants of standard Intruder Detection Systems (IDS) but with more of a focus on information gathering and deception.

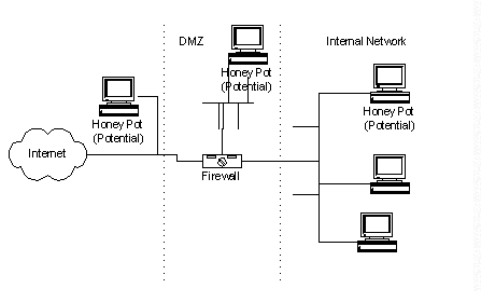

Fig.1: Honeypots installed in Internet Security system.

An example of a Honey Pot systems installed in a traditional Internet security design is shown in Figure 1.

Honey Pot system is setup to be easier prey for intruders but with minor system modifications so that their activity can be logged of traced. The general thought is that once an intruder breaks into a system, they will come back for subsequent visits. During these subsequent visits, additional information can be gathered and additional attempts at file, security and system access on the Honey can be monitored and saved[3]. A honey pot is a system that's put on a network so it can be probed and attacked. Because the honeypot has no production value, there is no "legitimate" use for it. This means that any interaction with the honeypot, such as a probe or a scan, is by definition suspicious.There are two types of honeypots:

- **Research**: Most attention to date has focused on research honeypots, which are used to gather information about the actions of intruders. For example, the Honey net Project is a volunteer, nonprofit security research organization that uses honeypots to collect information on cyber threats.
- **Production**: Less attention has been paid to production honeypots, which are actually used to protect organizations. Increasingly, however, production honeypots are being recognized for the detection capabilities they can provide and for the ways they can supplement both network- and host-based intrusion protection.

Why to set up Honey pot?

To learn how intruders probe and attempt to gain access to your systems. The general idea is that since a record of the intruder's activities is kept, you can gain insight into attack methodologies to better protect your real production systems.

Gather forensic information required to aid in the apprehension or prosecution of intruders. This is the sort of information often needed to provide law enforcement officials with the details needed to prosecute.

How to track intruder using Honeypots:

The information provided on an intruder depends on the levels of tracking that you've enabled on your Honey Pot.

Common tracking levels include the firewall, system logs on the Honey Pot and sniffer-based tools.

Firewall Logs

Firewalls are useful as part of the overall Honey Pot design for many reasons. Most fir`ewalls provide activity-logging capabilities which can be used to identify how an intruder is attempting to get into a Honey Pot. I liken firewall logs to router logs; they can both be set to trap and save packets of a pre-determined type. Remember that when setting up the firewall, you would normally want to log ALL packets going to the Honey Pot system, as there should be no legitimate reason for traffic going to or from the Honey Pot. Reviewing the order, sequence, time stamps and type of packets used by an intruder to gain access to you Honey Pot will help you identify the tools, methodology being used by the intruder and their intentions (vandalism, data theft, remote launch point search, etc.). Depending on the detail capabilities of logging on your firewall you may or not be able to gain considerable information from these logs.

Another useful function of many firewalls is their notification capabilities. Most firewalls can be configured to send alerts by email or pager to notify you of traffic going to or from your Honey Pot. This can be extremely useful in letting you review intruder activity WHILE it's happening.

System Logs

UNIX and Microsoft NT seem to have the lion share of the Internet server markets. Luckily, both operating systems have logging capabilities built into their operating systems, which help identify what changes or attempts have been made. It should be noted that out-of-the box, Unix offers superior logging capabilities as compared to Microsoft NT. Some of their out-of-the box logging capabilities include:

- Microsoft NT
  - ✓ Security – Available from Event Viewer
  - ✓ User Management – Needs to be enabled through User Manager
  - ✓ Running Services – Netsvc.exe needs to be manually run and compared to baseline.
- Unix
  - ✓ User activity logs – utmp, wtmp, btmp, lastlog, messages
  - ✓ Syslogd – An important option is that it can log to a remote server! The range of facilities and priorities available through syslogd is very good.

There are also several tools available that greatly increase the information that can be gathered. Many of the UNIX tools are public domain, while many of the Microsoft NT tools are not.

Sniffer Tools

Sniffer tools provide the capability of seeing all of the information or packets going between the firewall and the Honey Pot system. Most of the sniffers available are capable of decoding common tcp packets such as Telnet, HTTP and SMTP. Using a sniffer tool allows you to interrogate packets in more detail to determine which methods the intruder is trying to use in much more detail than firewall or system logging alone. An additional benefit to sniffer tools is that they can also create and store log files. The log files can then be stored and used for forensic purposes.

Building a Honey Pot

There is a variety of public domain tools and software available that can be useful to help you setup a Honey Pot as well as many sites dedicated to helping guide you through the process. Most tools seem to have originated on the Unix platform, while many have been ported to Microsoft NT.

What you will need to create or develop your own Honey Pot system are a minimum of the following components and considerable configuration time:

- A Workstation or PC. It appears as though an Intel-based workstation is fine.
- An operating system. I prefer BSD Unix or RedHat as there are more tools available for the UNIX platform than NT.
- Sniffer package.

II. COMMERCIAL HONEY POT SYSTEMS

There are a variety of commercial Honey Pot systems available. The operating systems most widely supported are Microsoft NT and UNIX. As many of the commercial products have been released in the past 12 – 18 months, some of them are still in relatively early versions. I tried to find information regarding market share but wasn't able to find any published statistics.

Some of the commercial Honey Pot systems available are:

- Network Associates, Cyber cop Sting
- Tripwire, Tripwire.
- Fred Cohen and Associates, Deception Toolkit.
- Recourse Technologies, Mantrap.

III. WORKING OF HONEY POT SYSTEM

Honey pots can also be described as being either low interaction or high interaction, a distinction based on the level of activity that the honeypot allows an attacker. A low-interaction system offers limited activity; in most cases, it works by emulating services and operating systems. The main advantages of low-interaction honeypots are that they are relatively easy to deploy and maintain and they involve minimal risk because an attacker never has access to a real operating system to harm others.

In contrast, high-interaction honey pots involve real operating systems and applications, and nothing is emulated. By giving attackers real systems to interact with, organizations can learn a great deal about an attacker's behavior. High-interaction honeypots make no assumptions about how an attacker will behave, and they provide an environment that tracks all activity. Such conditions allow organizations to learn about behavior they would not otherwise have access to.

High-interaction systems are also flexible, and IT security professionals can implement as much or as little of them as they want. In addition, this type of honeypot provides a more realistic target, capable of detecting a higher caliber of attacker. High-interaction honeypots can be complex to deploy, however, and they require additional technologies to prevent attackers from using the honeypot to launch attacks on other Systems [2].

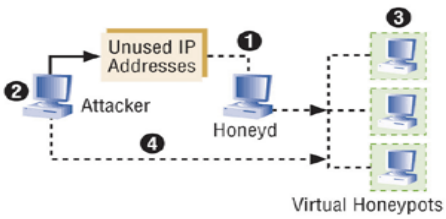

Fig.2: Honeyd Monitors[2]

The honeyd monitors are shown in figure 2, as when an attacker (2) probes an unused IP, Honeyd detects the probe, takes over that IP via ARP spoofing, then creates a virtual honeypot.(3) for the attacker to interact with (Honeyd can create multiple virtual honeypots to fool attackers on all unused addresses).The attacker is fooled into thinking he is interacting with a successful hacked system(4).In addition, honeyd automatically updates its list of unused IPs as systems are added or removed from the network.

- One solution being developed is the open-source Honeyd, which monitors unused IP space, instead of a single IP address. Any traffic or connection attempt made to an unassigned IP address is most likely unauthorized or illicit activity. This exponentially increases a honey pot's ability to detect unauthorized activity.
- When someone attempts to communicate with an unused IP, Honeyed--which is installed on a single computer--creates a virtual honeypot that interacts with the attacker. Honeyed also has the capability to detect activity on any TCP/UDP port, even if the connection is encrypted or uses IPv6 to tunnel traffic.

Honey pot Farms

While developments such as Honeyed address the scalability issue to some extent, honeypot farms promise to be a breakthrough technology.

- In the future, organizations won't deploy honeypots on their networks. Instead, they'll simply deploy a hardware device that monitors unused IP addresses, similar to Honeyed, and redirects all attacker traffic to a single cluster of honeypots (in Figure 3).

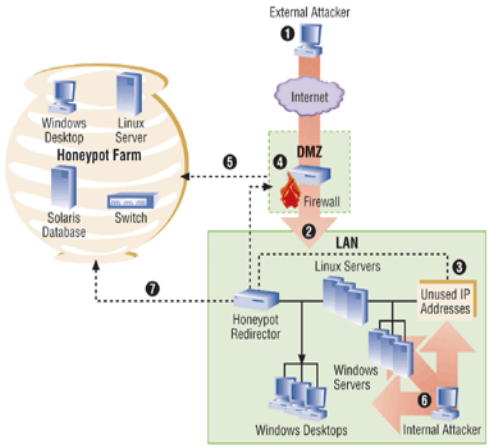

Fig.3: Schematic diagram for Honeypot farm[2]

In a scenario shown in Figure 3, an external attacker (1) penetrates the DMZ and scans network IP addresses (2). The redirection appliance (3) monitors all unused addresses, and uses Layer 2 VPN technology to enable the firewall (4) to redirect the intruder to the honeypot farm (5), which may have honeypot computers mirroring all types of real network devices. Similarly, an internal attacker (6), scanning the network for vulnerable systems such as open file shares is redirected (7) by the honeypot appliance when he probes unused IP addesses.

- Centralizing the hardware solves the problem of deploying and maintaining honeypots on the network. In fact, we're likely to see this offered as a service,

with managed security service providers (MSSPs) maintaining farms for clients.

- Honeypot farms will simplify administration--all your honeypots will be in one location, where they can be monitored. For example, a major auto manufacturer wants to deploy honeypots on all of its networks around the world. That's a logistical nightmare. But with farms, all the honeypots are physically located at the company's headquarters and maintained by security specialists. Admin will simply deploy devices on the local networks to redirect unauthorized traffic to the farm.
- Instead of bringing the honeypot to the attacker, attackers in the future will be directed to the honeypot.
- We're already seeing this in such commercial solutions as NetBait. NetBait provides a service where it will deploy redirectors on your internal network. Attackers are then redirected to NetBait's honey pot farm, where their every action is detected and recorded. Or, if an organization prefers, it can maintain its own honeypot farm, using the NetBait solution to redirect attackers.

Advantages of honey pots

Security experts say that honeypots can succeed in a number of areas where traditional intrusion-detection systems (IDS) have been found wanting. The main advantages are:

- Too much data: One of the common problems with the traditional IDS is that it generates a huge amount of alerts. The sheer volume of this "noise" makes it time-consuming, resource-intensive and costly to review the data. In contrast, 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 unauthorized activity.
- False positives: Perhaps the biggest drawback of IDS is that so many of the alerts generated are false. False positives are a big problem even for organizations that spend a lot of time tuning their systems. If IDS continually creates false positives, administrators may eventually begin to ignore the system. Honeypots sidestep this problem because any activity with them is, by definition, unauthorized. That allows organizations to reduce, if not eliminate, false alerts.
- False negatives: IDS technologies can also have difficulty identifying unknown attacks or behavior. Again, any activity with a honeypot is anomalous, making new or previously unknown attacks stand out.
- Resources: An ID requires resource-intensive hardware to keep up with an organization's network traffic. As a network increases in speed and generates more data, the IDS have to get bigger to keep up. Honeypots require minimal resources, even on large networks. According to Lance Spitzner, founder of the Honey net Project, a single Pentium computer with 128MB of RAM can be used to monitor millions of IP addresses.
- Encryption: More organizations are moving to encrypt all their data, either because of security issues or regulations, such as the Health Insurance Portability and Accountability Act. Not surprisingly, 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 an attacker is using encryption; the activity will still be captured.

Honey pots have their advantages and disadvantages[3]. They are clearly a useful tool for luring and trapping attackers, capturing information and generating alerts when someone is interacting with them. The activities of attackers provide valuable information for analyzing their attacking techniques and methods. Because honeypots only capture and archive data and requests coming in to them, they do not add extra burden to existing network bandwidth.

However, honeypots do have their drawbacks. Because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in the n network. Furthermore, deploying honeypots without enough planning and consideration may introduce more risks to an existing network, because honeypots are designed to be exploited, and there is always a risk of them being taken over by attackers, using them as a stepping-stone to gain entry to other systems within the network. This is perhaps the most controversial drawback of honey pots.

How honeypots augment IDSs

The evolution of honeypots can also be understood by looking at the ways these systems are being used in association with IDSs to prevent, detect and help respond to attacks. Indeed, honeypots are increasingly finding their place alongside network- and host-based intrusion-protection systems[4].

Honeypots are able to prevent attacks in several ways. The first is by slowing down or stopping automated attacks, such as worms or auto rooters[9]. These are attacks that randomly scan an entire network looking for vulnerable systems. (Honeypots use a variety of TCP tricks to put an attacker in a "holding pattern.") The second way is by

deterring human attacks. Here honeypots aim to sidetrack an attacker, making him devote attention to activities that cause neither harm nor loss while giving an organization time to respond and block the attack.

As noted above, honeypots can provide early detection of attacks by addressing many of the problems associated with traditional IDSs, such as false positives and the inability to detect new types of attacks, or zero-day attacks. But increasingly, honeypots are also being used to detect insider attacks, which are usually more subtle and more costly than external attacks.

Detection methodology

Honey pots can fill the growing gaps which suffer from false positives and a lack of alert intelligence. As a result, we're going to see much wider deployments in the next few years. That's not to say honey pots will replace IDSes. Each technology has its strengths and limitations.

We are already beginning to see this technology. Symantec's honeypot, Decoy Server, works with the company's IDS solution, Manhunt. Decoy Server is an advanced honeypot that doesn't emulate services; instead, it creates multiple instances of real operating systems. Attackers then interact with these real operating systems and applications. This information is fed into a central system, where it's combined with data from Manhunt[5].

Honey pots are also helping organizations respond to attacks. A hacked production system can be difficult to analyze, since it's hard to determine what normal day-to-day activity is and what intruder activity is. Honeypots, by capturing only unauthorized activity, can be effective as an incident-response tool because they can be taken off-line for analysis without affecting business operations[8]. The newest honeypots boast stronger threat-response mechanisms, including the ability to shut down systems based on attacker activity and frequency-based policies that enable security administrators to control the actions of an attacker in the honeypot.

Potential issues with honey pots

Secrecy is paramount when deploying a honey pot or honey net. If everyone knows it is a trap, no-one will attempt to attack it at all, except perhaps automated tools such as worms. Some honeypots, especially low interaction ones, may be easily identified as honeypots by an attacker due to their emulation of services. Any emulation of a complex system will always differ from the real thing; for example, there are a variety of ways for a program to check if it is running within a virtual machine and malware is increasingly using these techniques to hamper analysis[6]. There will always be an arms race between those trying to develop ways of detecting honeypots, and those who are trying to improve honeypots so they are harder to fingerprint.

Client-side attack frameworks exist, such as MPack that contain automated mechanisms that make detection and analysis of malicious web servers with client honeypots more difficult. For example, client-side attacks might not trigger if the client honeypot accesses a malicious web server from a specific network (for example, from our research lab) and/or client-side attacks might only trigger once. Upon repeated interaction, the malicious web server might not launch client-side attacks anymore making tracking and analysis of the malicious server and its attack difficult.

Another concern is that if a high interaction honeypot is compromised, the attacker may attempt to use this as a stepping stone to damage or take over other systems[7]. Ideally the honeypot should use several mechanisms to prevent this, and the operator should pay close attention so no harm comes to innocent third-parties. In some jurisdictions, legal liability for the actions of users of the honeypot may be a concern, as May local electronic interception laws.

IV. CONCLUSION

Like all technologies, honeypots have their drawbacks, the greatest one being their limited field of view. Honeypots capture only activity that's directed against them and will miss attacks against other systems. For that reason, security experts don't recommend that these systems replace existing security technologies. Instead, they see honeypots as a complementary technology to network- and host-based intrusion protection. The advantages that honey pots bring to intrusion-protection solutions are hard to ignore, especially now as production honeypots are beginning to be deployed. In time, as deployments proliferate, honeypots could become an essential ingredient in an enterprise-level security operation.

REFERENCES

[1] Honey Pot Systems Explained, Loras R. Even, July 12, 2000.
[2] Honeypot technology: How honeypot work in the enterprise,Lance Spitzer,2001-2015.
[3] Honeypots: The sweet spot in network security, By John Harrison, Symantec Corp.
[4] HONEYPOT SECURITY February2008, http://www.iosec.gov.hk/english/technical/files/honeypots.pdf

[5] A Guide to Different Kinds of Honeypots, Jamie Riden and Christian Seifert, 13 Feb 2008][[Spitzner02] Spitzner, L. Honeypots: Tracking Hackers, Addison-Wesley, Boston, 2002.]
[6] Honeynet Project, "Know Your Enemy: A Forensic Analysis". 2002. Available on line at: http://project.honeynet.org/papers/index.html]).
[7] L. Spitzner, Honeypots: tracking hackers. Vol. 1. Reading: Addison-Wesley, 2003.
[8] .D. Powell, "Failure Mode Assumptions and Assumption Coverage: A Revised Version", LAAS-CNRS, France. Research Report 91462.]
[9] F. Pouget, M. Dacier, "Honeypot, Honeynet: A comparative survey". Eurecom Research Report RR-03-082. August 2003.